

SMALL VALUE ESTIMATES FOR THE MULTIPLICATIVE GROUP

DAMIEN ROY

ABSTRACT. We generalize Gel'fond's transcendence criterion to the context of a sequence of polynomials whose first derivatives take small values on large subsets of a fixed subgroup of the multiplicative group \mathbb{C}^\times of \mathbb{C} .

1. INTRODUCTION

For applications to transcendental number theory, it would be desirable to extend the actual criteria for algebraic independence so that they deal more efficiently with polynomials taking small values on large subsets of a finitely generated subgroup of an algebraic group. At the moment, one could say that these criteria concentrate on the smallest non-zero value of each polynomial on such sets, regardless of the global distribution of values. A good illustration of the need for refined criteria, and our main motivation for this quest, is a conjectural small value estimate for the algebraic group $\mathbb{G}_a \times \mathbb{G}_m$ which is proposed in [6] and shown to be equivalent to Schanuel's conjecture. In a preceding paper [7], we explored the case of the additive group \mathbb{G}_a . Here, we turn to the multiplicative group \mathbb{G}_m . Although this is again an algebraic group of dimension one, we will see that it presents new challenges as roots of unity come into play.

Let \mathbb{C}^\times denote the multiplicative group of non-zero complex numbers, let m be a positive integer, and let $\xi_1, \dots, \xi_m \in \mathbb{C}^\times$. An application of Dirichlet's box principle shows that, for any non-negative real numbers β, σ, τ and ν with

$$(1) \quad m\sigma + \tau < 1, \quad \beta > (m+1)\sigma + \tau \quad \text{and} \quad \nu < 1 + \beta - m\sigma - \tau,$$

and for any positive integer n which is sufficiently large in terms of the preceding data, there exists a non-zero polynomial $P \in \mathbb{Z}[T]$ of degree at most n and height at most $\exp(n^\beta)$ satisfying $|P^{[j]}(\xi_1^{i_1} \dots \xi_m^{i_m})| < \exp(-n^\nu)$ for each choice of integers i_1, \dots, i_m and j with $0 \leq i_1, \dots, i_m \leq n^\sigma$ and $0 \leq j < n^\tau$. Here the *height* of P , denoted $H(P)$, is defined as the maximum of the absolute value of its coefficients divided by their greatest common divisor, and the expression $P^{[j]}$ stands for the j -th divided derivative of P (see §2). The goal of this paper is to establish the following partial converse to this statement.

1991 *Mathematics Subject Classification.* Primary 11J85; Secondary 11J81.
Work partially supported by NSERC and CICMA.

Theorem 1.1. *Let m be a positive integer, let ξ_1, \dots, ξ_m be non-zero multiplicatively independent complex numbers which generate over \mathbb{Q} a field of transcendence degree one, and let $\beta, \sigma, \tau, \nu \in \mathbb{R}$ with*

$$(2) \quad \sigma \geq 0, \quad \tau \geq 0, \quad \frac{5m+1}{m+5}\sigma + \tau < 1, \quad \beta \geq 1 + \sigma,$$

$$(3) \quad \nu > \begin{cases} 1 + \beta - \frac{3m-1}{m+5}\sigma - \tau & \text{if } m \geq 2, \\ 1 + \beta - \frac{5}{11}\sigma - \tau & \text{if } m = 1. \end{cases}$$

Then, for infinitely many positive integers n , there exists no non-zero polynomial $P \in \mathbb{Z}[T]$ with $\deg(P) \leq n$ and $H(P) \leq \exp(n^\beta)$ such that

$$(4) \quad \max \{ |P^{[j]}(\xi_1^{i_1} \cdots \xi_m^{i_m})| ; 0 \leq i_1, \dots, i_m \leq n^\sigma, 0 \leq j < n^\tau \} < \exp(-n^\nu).$$

When $m = 1$ and $\sigma = \tau = 0$, the above result reduces to the well-known Gel'fond's transcendence criterion. So, for $m = 1$, it provides a gain of $(5/11)\sigma + \tau$ in the estimate for ν compared to Gel'fond's criterion. For $m \geq 2$, the gain is $((3m-1)/(m+5))\sigma + \tau$. On the other hand, the conditions (1) of application of Dirichlet's box principle put an upper bound on the gain that can be achieved. It suggests the possibility that Theorem 1.1 remains true for any integer $m \geq 1$ with the condition on ν relaxed to $\nu > 1 + \beta - m\sigma - \tau$, when $m\sigma + \tau < 1$, but we have not been able to prove this. Note that, when $\sigma = 0$, Theorem 1.1 deals with finitely many points and then it follows from Proposition 1 of [5]. The novelty here is that we deal with large numbers of points.

The proof of the above result is involved but the main underlying idea is simple and is inspired by techniques from zero estimates. If a polynomial $P \in \mathbb{Z}[T]$ takes small values at all points of the form ξ^a with ξ in a subset E of \mathbb{C}^\times and a in a subset A of \mathbb{N}^* , then the polynomials $P(T^a)$ with $a \in A$ take small values at all points of E . Applying Corollary 3.2 of [7], one deduces that the product $\prod_{\xi \in E} |Q(\xi)|$ is small, where $Q(T)$ denotes the greatest common divisor in $\mathbb{Z}[T]$ of the polynomials $P(T^a)$ with $a \in A$. However, for this to be useful, we also need good upper bounds for the degree and height of $Q(T)$. The precise result that we use for this purpose is stated and proved in Section §7. For simplicity, we just mention here the following consequence of it, where $\mathbb{C}_{\text{tor}}^\times$ stands for the group of roots of unity, the torsion part of \mathbb{C}^\times .

Theorem 1.2. *Let $\beta, \delta, \mu \in \mathbb{R}$ with $0 < \delta$, $0 < \mu < 1$ and $1 + \mu < \beta$. Let n be a positive integer, let A be the set of all prime numbers p with $p \leq n^\mu$, let P be a non-zero polynomial of $\mathbb{Z}[T]$ of degree at most n and height at most $\exp(n^\beta)$ with no root in $\mathbb{C}_{\text{tor}}^\times \cup \{0\}$, and let $Q \in \mathbb{Z}[T]$ be a greatest common divisor of the polynomials $P(T^a)$ with $a \in A$. If n is sufficiently large as a function of β , δ and μ , we have $\deg(Q) \leq n^{1-\mu+\delta}$ and $H(Q) \leq \exp(n^{\beta-2\mu+\delta})$.*

This result is the multiplicative analog of Theorem 1.2 of [7]. To achieve such non-trivial estimates on the degree and height of Q , the requirement that P has no root in $\mathbb{C}_{\text{tor}}^\times \cup \{0\}$ is necessary. For example, if $P(T)$ is of the form $T^r(T^s - 1)$ for some integers $r \geq 0$ and $s \geq 1$, then $P(T)$ divides $P(T^a)$ for any integer $a \geq 1$, and so $P(T)$ itself is the gcd of the latter collection of polynomials.

In practice, we start with a polynomial P satisfying (4) and we take for E a suitable subset of the subgroup of \mathbb{C}^\times generated by ξ_1, \dots, ξ_m . In order to get appropriate degree and height estimates for the corresponding polynomial Q , we first need to remove from P a suitable cyclotomic factor. General estimates for this are given in §3. They require a lower bound for the absolute value of the cyclotomic factor on the set E . This is easy to achieve if one assumes that ξ_1, \dots, ξ_m do not all have absolute value one, but the general case requires more elaborate arguments which occupy all of §4 and §5 for the case $m \geq 2$, and most of §9 in the case $m = 1$. The proof of Theorem 1.1 is completed in §8 for $m \geq 2$ and in §11 for $m = 1$. In both case, we end up with a product $\prod_{\xi \in E} |Q(\xi)|$ being small and we need to choose $\xi \in E$ such that $|Q(\xi)|$ is small in order to be able to apply a standard transcendence criterion. The refined estimate that we obtain in the case $m = 1$ follows by observing that these values $|Q(\xi)|$ cannot be uniformly small. For this we use a combinatorial result proved in §10 as an extension of Proposition 9.1 of [7].

2. NOTATION AND PRELIMINARIES

Throughout this paper, the symbols i, j, k are restricted to integers. We denote by \mathbb{C}^\times the multiplicative group of non-zero complex numbers, by $\mathbb{C}_{\text{tor}}^\times$ its torsion subgroup, by \mathbb{N} the set of non-negative integers, and by \mathbb{N}^* the set of positive integers. We also denote by $|E|$ the cardinality of an arbitrary set E , and by ϕ the Euler totient function. A *cyclotomic* polynomial is a monic polynomial of $\mathbb{Z}[T]$ whose roots lie in $\mathbb{C}_{\text{tor}}^\times$. For any integer $j \geq 0$, we define the j -th *divided* derivative of a polynomial $P \in \mathbb{C}[T]$ by $P^{[j]} = (j!)^{-1} P^{(j)}$ where $P^{(j)} = d^j P / dT^j$ is the usual j -th derivative of P . Finally, the *length* $L(P)$ of a polynomial $P \in \mathbb{C}[T_1, \dots, T_m]$ is the sum of the absolute values of its coefficients.

Let K be a number field and let $d = [K : \mathbb{Q}]$. For each place v of K , we normalize the corresponding v -adic absolute value $|\cdot|_v$ of K so that it extends the usual absolute value of \mathbb{Q} if v is Archimedean, or the usual p -adic absolute value of \mathbb{Q} with $|p|_v = p^{-1}$ if v lies above a prime number p . We also denote by K_v the completion of K at v , and by d_v its local degree. For any polynomial $P \in K_v[T_1, \dots, T_m]$, we define the v -adic norm $\|P\|_v$ of P as the largest v -adic absolute value of its coefficients. Finally we define the *height* $H(P)$ of any polynomial $P \in K[T_1, \dots, T_m]$ by

$$H(P) = \prod_v \|P\|_v^{d_v/d}$$

where the product extends over all places v of K . This height is said to be *homogeneous* because it satisfies $H(aP) = H(P)$ for any non-zero element a of K , and *absolute* as it is independent of the choice of the number field K containing the coefficients of P . It therefore extends to a height on $\overline{\mathbb{Q}}[T_1, \dots, T_m]$ where $\overline{\mathbb{Q}}$ stands for the algebraic closure of \mathbb{Q} . In particular, the height of a non-zero polynomial $P \in \mathbb{Z}[T_1, \dots, T_m]$ is simply given by $H(P) = \|P\| / \text{cont}(P)$ where $\|P\| = \|P\|_\infty$ is the maximum of the absolute values of its coefficients (we also use the latter notation for polynomials with complex coefficients), and where the *content* $\text{cont}(P)$ of P is the gcd of its coefficients. We say that a non-zero polynomial of $\mathbb{Z}[T_1, \dots, T_m]$ is *primitive* if its content is 1, and that it is *primary* if it is a power of an irreducible element of $\mathbb{Z}[T_1, \dots, T_m]$. This implies that a non-constant primary polynomial of $\mathbb{Z}[T_1, \dots, T_m]$ is primitive.

In the sequel, we will frequently use the well-known fact that for one-variable polynomials $P_1, \dots, P_s \in \overline{\mathbb{Q}}[T]$ with product $P = P_1 \cdots P_s$, we have

$$(5) \quad e^{-\deg(P)} H(P) \leq H(P_1) \cdots H(P_s) \leq e^{\deg(P)} H(P).$$

For a single point $x \in \overline{\mathbb{Q}}$, we use the same notation $H(x)$ to denote the *inhomogeneous height* of x , that is the height of the polynomial $T - x$. For $x \in K$, it is given by the formula $H(x) = \prod \max\{1, |x|_v\}^{d_v/d}$ where the product runs through all places v of K . As the field K can be chosen to be arbitrarily large, this shows that we have $H(x^m) = H(x)^{|m|}$ for any $m \in \mathbb{Z}$ and any non-zero $x \in \overline{\mathbb{Q}}$. From (5), we deduce that, if $x_1, \dots, x_s \in \overline{\mathbb{Q}}$ are all the roots of a non-zero polynomial $P \in \overline{\mathbb{Q}}[T]$ of degree s , listed with their multiplicities, we have

$$(6) \quad e^{-s} H(P) \leq H(x_1) \cdots H(x_s) \leq e^s H(P).$$

The following lemma formalizes the standard procedure of “linearization” while handling multiplicities at the same time (cf. [7, Lemma 2.1]).

Lemma 2.1. *Let $\varphi: \mathbb{Z}[T] \rightarrow [0, \infty)$ be a multiplicative function, let δ , d and Y be positive real numbers with $\delta < 1$ and $e^d \leq Y$, and let $t \in \mathbb{N}^*$. Suppose that there exists a non-zero polynomial $Q_1 \in \mathbb{Z}[T]$ of degree at most d and height at most Y for which $Q = \gcd\{Q_1^{[j]}(T); 0 \leq j < t\}$ satisfies $\varphi(Q) \leq \delta$. Then, there exists a primary polynomial $S \in \mathbb{Z}[T]$ with*

$$\deg(S) \leq d/t, \quad H(S) \leq Y^{2/t} \quad \text{and} \quad \varphi(S) \leq \delta^{1/(6t)}.$$

By *multiplicative*, we mean that the function φ satisfies $\varphi(FG) = \varphi(F)\varphi(G)$ for any $F, G \in \mathbb{Z}[T]$. In our applications later, φ takes the form $\varphi(P) = \prod_{\xi \in E} |P(\xi)|$ for some fixed finite set of complex numbers E .

Proof. Let $Q = R_1 \cdots R_s$ be a factorization of Q into irreducible elements of $\mathbb{Z}[T]$. Since Q divides Q_1 , we find

$$\prod_{i=1}^s \left(Y^{\deg(R_i)} H(R_i)^d \right) \leq Y^{\deg(Q_1)} \left(e^{\deg(Q_1)} H(Q_1) \right)^d \leq Y^{3d}.$$

Therefore, upon writing $\delta = Y^{-3d\eta}$ for an appropriate value of $\eta > 0$, we obtain

$$\prod_{i=1}^s \varphi(R_i) = \varphi(Q) \leq Y^{-3d\eta} \leq \prod_{i=1}^s \left(Y^{\deg(R_i)} H(R_i)^d \right)^{-\eta}.$$

So, there is at least one index i with $1 \leq i \leq s$ such that the polynomial $R = R_i$ satisfies

$$(7) \quad \varphi(R) \leq \left(Y^{\deg(R)} H(R)^d \right)^{-\eta}.$$

Since R divides $Q_1^{[j]}$ for $j = 0, \dots, t-1$, the polynomial Q_1 is divisible by R^t . This implies that $\deg(R) \leq d/t$ and $H(R)^t \leq e^d H(Q_1) \leq Y^2$. Let $k \geq 1$ be the largest integer such that the polynomial $S = R^k$ satisfies $\deg(S) \leq d/t$ and $H(S) \leq Y^{2/t}$ (such an integer exists since $R \neq \pm 1$). We consider two cases. If $\deg(S) \geq d/(2t)$, then (7) leads to $\varphi(S) \leq Y^{-\eta \deg(S)} \leq Y^{-\eta d/(2t)} = \delta^{1/(6t)}$. On the other hand, if $\deg(S) < d/(2t)$, we have $\deg(R^{2k}) \leq d/t$ and so $H(R^{2k}) \geq Y^{2/t}$. As $H(R^{2k}) \leq e^{\deg(R^{2k})} H(R)^{2k} \leq Y^{1/t} H(R)^{2k}$, we deduce that $H(R)^k \geq Y^{1/(2t)}$ and then (7) leads to $\varphi(S) \leq H(R)^{-\eta kd} \leq Y^{-\eta d/(2t)} = \delta^{1/(6t)}$, as in the previous case. \square

For any finite subset E of \mathbb{C} with at least two points, we define

$$(8) \quad \Delta_E = \prod_{\xi' \neq \xi} |\xi' - \xi|^{1/2}$$

where the product is taken over all ordered pairs (ξ, ξ') of distinct elements of E . When E consists of one point, we put $\Delta_E = 1$. The following result is a reformulation of Corollary 3.2 of [7] and our main tool to study families of polynomials taking small values on such a set E .

Proposition 2.2. *Let E be a non-empty finite set of complex numbers, let $n, t \in \mathbb{N}^*$ with $n \geq t|E|$, let $P_1, \dots, P_r \in \mathbb{Z}[T]$ be a finite sequence of $r \geq 2$ non-zero polynomials of degree at most n , and let $Q \in \mathbb{Z}[T]$ be their greatest common divisor. Then we have*

$$(9) \quad \prod_{\xi \in E} \left(\frac{|Q(\xi)|}{\text{cont}(Q)} \right)^t \leq c_1 \left(\max_{1 \leq i \leq r} H(P_i) \right)^{2n} \prod_{\xi \in E} \left(\max_{\substack{1 \leq i \leq r \\ 0 \leq j < t}} |P_i^{[j]}(\xi)| \right)^t,$$

with $c_1 = e^{10n^2} (2 + c_E)^{4nt|E|} \Delta_E^{-t^2}$, where $c_E = \max_{\xi \in E} |\xi|$ and Δ_E is defined by (8).

We conclude this section by stating the version of Gel'fond's criterion on which all our results ultimately rely. It is mainly due to Brownawell [1] and Waldschmidt [9] (see the comments after Lemma 2.2 of [7] for more details).

Lemma 2.3. *Let α, β and ϵ be positive real numbers with $\beta \geq \alpha$, and let ξ_1, \dots, ξ_m be a finite sequence of complex numbers which generate a field of transcendence degree one over \mathbb{Q} . For infinitely many integers n , there exists no polynomial $P \in \mathbb{Z}[T_1, \dots, T_m]$ of degree at most n^α and height at most $\exp(n^\beta)$ satisfying*

$$0 < |P(\xi_1, \dots, \xi_m)| \leq \exp(-n^{\alpha+\beta+\epsilon}).$$

3. THE FIRST STEP

The goal of this section is to establish the following result which represents the first step in the proof of our main theorem.

Proposition 3.1. *Let $M, n, t \in \mathbb{N}^*$ and $X \in \mathbb{R}$ with $1 \leq t \leq n$. Let A be a non-empty subset of $\{1, 2, \dots, M\}$, and let E be a non-empty finite subset of \mathbb{C}^\times with $E \cap \mathbb{C}_{\text{tor}}^\times = \emptyset$. Finally, let $P \in \mathbb{Z}[T]$ be a non-zero polynomial with $\deg(P) \leq n$ and $H(P) \leq X$, written as a product $P(T) = P_0(T)T^r\Phi(T)^t$ where $P_0 \in \mathbb{Z}[T]$, $r \in \mathbb{N}$ and $\Phi \in \mathbb{Z}[T]$, with Φ cyclotomic. Put*

$$\begin{aligned} c_E &= \max\{\max(|\xi|, |\xi|^{-1}); \xi \in E\}, \\ \delta_\Phi &= \min\{|\Phi(\xi^a)|; a \in A, \xi \in E\}, \\ \delta_P &= \max\{|P^{[j]}(\xi^a)|; a \in A, \xi \in E, 0 \leq j < 2t - 1\}, \end{aligned}$$

and assume that

$$(10) \quad t|E| \leq Mn \leq \frac{1}{10} \log X \quad \text{and} \quad (2 + c_E)^{20t|E|} \leq X.$$

Then the polynomial $Q(T) = \gcd\{P_0^{[j]}(T^a); a \in A, 0 \leq j < t\}$ (computed in $\mathbb{Z}[T]$) satisfies

$$\prod_{\xi \in E} \frac{|Q(\xi)|}{\text{cont}(Q)} \leq X^{5Mn/t} \Delta_E^{-t} \left(\frac{\delta_P}{\min(1, \delta_\Phi)^{3t}} \right)^{|E|}.$$

In practice, given P , we choose r to be the largest non-negative integer such that T^r divides $P(T)$, and $\Phi(T)$ to be the cyclotomic polynomial of $\mathbb{Z}[T]$ of largest degree such that $\Phi(T)^t$ divides $P(T)$. Then, we have $Q(0) \neq 0$ and no root of Q is a root of unity. As we saw in §1, such conditions are required in order to get good estimates on the degree and height of Q .

To prove the above result, we will apply Proposition 2.2 to the family of polynomials $P_0^{[j]}(T^a)$ with $a \in A$ and $0 \leq j < t$. In order to estimate the absolute value of their derivatives at the elements of E , we first establish three lemmas.

Lemma 3.2. *Let $\Phi \in \mathbb{C}[T]$, $t \in \mathbb{N}^*$ and $\xi \in \mathbb{C}$ with $\Phi(\xi) \neq 0$. For any integer $j \geq 0$, we have*

$$\left| (\Phi^{-t})^{[j]}(\xi) \right| \leq \frac{1}{j!} \left((t + 2j) \deg(\Phi) \|\Phi\| \max(1, |\xi|)^{\deg(\Phi)} \right)^j |\Phi(\xi)|^{-t-j}.$$

Proof. For each $j \geq 0$, the j -th derivative of Φ^{-t} can be written in the form $(\Phi^{-t})^{(j)} = A_j \Phi^{-t-j}$ where A_j is a polynomial of $\mathbb{C}[T]$ satisfying $A_0 = 1$ for $j = 0$, and the recurrence relation $A_j = A'_{j-1} \Phi - (t+j-1)A_{j-1} \Phi'$ for $j \geq 1$. If $j \geq 1$, this gives $\deg(A_j) \leq \deg(A_{j-1}) + \deg(\Phi)$ and by recurrence we get $\deg(A_j) \leq j \deg(\Phi)$ for each $j \geq 0$. For the length of these polynomials, we also find, for $j \geq 1$,

$$\begin{aligned} L(A_j) &\leq L(A'_{j-1}) \|\Phi\| + (t+j-1) L(A_{j-1}) \|\Phi'\| \\ &\leq (\deg(A_{j-1}) + (t+j-1) \deg(\Phi)) \|\Phi\| L(A_{j-1}) \\ &\leq (t+2j-2) \deg(\Phi) \|\Phi\| L(A_{j-1}), \end{aligned}$$

which by recurrence gives $L(A_j) \leq ((t+2j) \deg(\Phi) \|\Phi\|)^j$. The conclusion follows using $|A_j(\xi)| \leq L(A_j) \max(1, |\xi|)^{\deg(A_j)}$. \square

Lemma 3.3. *Let $n, t \in \mathbb{N}^*$ with $1 \leq t \leq n$, and let $P \in \mathbb{Z}[T]$ be a non-zero polynomial of degree at most n . Suppose that P factors as a product $P(T) = P_0(T) T^r \Phi(T)^t$ where $P_0 \in \mathbb{Z}[T]$, $r \in \mathbb{N}$ and $\Phi \in \mathbb{Z}[T]$, with Φ cyclotomic. Then, for each $\xi \in \mathbb{C}^\times$ with $\Phi(\xi) \neq 0$, we have*

$$\max_{0 \leq j < 2t-1} |P_0^{[j]}(\xi)| \leq e^{10n} \max(|\xi|, |\xi|^{-1})^{3n} \min(1, |\Phi(\xi)|)^{-3t} \max_{0 \leq j < 2t-1} |P^{[j]}(\xi)|.$$

Proof. Since $P_0(T) = P(T) T^{-r} \Phi(T)^{-t}$, Leibniz' formula for the derivative of a product gives, for each integer $j \geq 0$,

$$(11) \quad P_0^{[j]}(T) = \sum_{j_0+j_1+j_2=j} P^{[j_0]}(T) (T^{-r})^{[j_1]} (\Phi(T)^{-t})^{[j_2]},$$

where the summation runs through all decompositions of j as a sum of non-negative integers j_0, j_1, j_2 . Let $\xi \in \mathbb{C}^\times$ with $\Phi(\xi) \neq 0$. As we have $r \leq n$ and $t \leq n$, we find, for each $j = 0, 1, \dots, 2t$,

$$\left| (T^{-r})^{[j]}(\xi) \right| = \binom{r+j-1}{j} |\xi|^{-r-j} \leq \frac{(3n)^j}{j!} \max(1, |\xi|^{-1})^{3n}.$$

Since Φ^t divides P , we have $\deg(\Phi) \leq n/t$, and since Φ is monic with all of its roots on the unit circle, we deduce that $\|\Phi\| \leq 2^{\deg(\Phi)} \leq 2^{n/t}$. Then, for $j = 0, 1, \dots, 2t$, Lemma 3.2 gives

$$\left| (\Phi^{-t})^{[j]}(\xi) \right| \leq \frac{(5n)^j}{j!} 2^{2n} \max(1, |\xi|)^{2n} \min(1, |\Phi(\xi)|)^{-3t}.$$

Combining these estimates with (11), we conclude that

$$\max_{0 \leq j < 2t-1} |P_0^{[j]}(\xi)| \leq C \max(|\xi|, |\xi|^{-1})^{3n} \min(1, |\Phi(\xi)|)^{-3t} \max_{0 \leq j < 2t-1} |P^{[j]}(\xi)|,$$

with

$$C = \sum_{j_1, j_2 \geq 0} \frac{(3n)^{j_1} (5n)^{j_2}}{j_1! j_2!} 2^{2n} \leq e^{10n}.$$

\square

Lemma 3.4. *Let $a, t \in \mathbb{N}^*$, $P \in \mathbb{Z}[T]$ and $F(T) = P(T^a)$. For each $\xi \in \mathbb{C}$, we have*

$$\max_{0 \leq j < t} |F^{[j]}(\xi)| \leq (2 + |\xi|)^{at} \max_{0 \leq j < t} |P^{[j]}(\xi^a)|.$$

Proof. Let $n = \deg(P)$. Expanding F and P in Taylor series around ξ and ξ^a respectively, we find

$$\sum_{j=0}^{an} F^{[j]}(\xi) T^j = F(T + \xi) = P((T + \xi)^a) = \sum_{j=0}^n P^{[j]}(\xi^a) ((T + \xi)^a - \xi^a)^j.$$

Since T^t divides $((T + \xi)^a - \xi^a)^j$ for each $j \geq t$, this shows that the polynomials

$$\sum_{j=0}^{t-1} F^{[j]}(\xi) T^j \quad \text{and} \quad \sum_{j=0}^{t-1} P^{[j]}(\xi^a) ((T + \xi)^a - \xi^a)^j$$

have the same coefficients of T^j for $j = 0, 1, \dots, t-1$. Therefore the length of the first is bounded above by that of the second, and so we obtain

$$\sum_{j=0}^{t-1} |F^{[j]}(\xi)| \leq \sum_{j=0}^{t-1} |P^{[j]}(\xi^a)| (1 + |\xi|)^{aj} \leq (2 + |\xi|)^{at} \max_{0 \leq j < t} |P^{[j]}(\xi^a)|.$$

□

Proof of Proposition 3.1. Fix temporarily a choice of $a \in A$, $\xi \in E$ and $k \in \mathbb{N}$ with $k < t$, and put $\tilde{P} = P_0^{[k]}(T^a)$. Since P_0 divides P and since $4n \leq \log X$ by (10), we find

$$(12) \quad \deg(\tilde{P}) \leq a \deg(P_0) \leq Mn \quad \text{and} \quad H(\tilde{P}) \leq 2^n H(P_0) \leq 2^n e^n X \leq X^{3/2}.$$

According to Lemma 3.4, we have

$$\max_{0 \leq j < t} |\tilde{P}^{[j]}(\xi)| \leq (2 + |\xi|)^{at} \max_{0 \leq j < t} |P_0^{[k][j]}(\xi^a)| \leq (2 + c_E)^{Mt} 2^{2t} \max_{0 \leq j < 2t-1} |P_0^{[j]}(\xi^a)|.$$

By Lemma 3.3, we also have

$$\begin{aligned} \max_{0 \leq j < 2t-1} |P_0^{[j]}(\xi^a)| &\leq e^{10n} \max(|\xi^a|, |\xi^a|^{-1})^{3n} \min(1, |\Phi(\xi^a)|)^{-3t} \max_{0 \leq j < 2t-1} |P^{[j]}(\xi^a)| \\ &\leq e^{10n} c_E^{3Mn} \min(1, \delta_\Phi)^{-3t} \delta_P. \end{aligned}$$

Combining the last two estimates and using $t \leq n \leq Mn$ and $e \leq 2 + c_E$, we obtain

$$(13) \quad \max_{0 \leq j < t} |\tilde{P}^{[j]}(\xi)| \leq (2 + c_E)^{16Mn} \min(1, \delta_\Phi)^{-3t} \delta_P.$$

With the estimates (12) and (13) at hand, we are now ready to apply Proposition 2.2 to the collection of polynomials $P_0^{[k]}(T^a)$ with $a \in A$ and $0 \leq k < t$. Using the hypotheses (10), it gives

$$\begin{aligned} \prod_{\xi \in E} \left(\frac{|Q(\xi)|}{\text{cont}(Q)} \right)^t &\leq e^{10(Mn)^2} (2 + c_E)^{4(Mn)t|E|} \Delta_E^{-t^2} (X^{3/2})^{2Mn} \left(\frac{(2 + c_E)^{16Mn} \delta_P}{\min(1, \delta_\Phi)^{3t}} \right)^{t|E|} \\ &\leq X^{5Mn} \Delta_E^{-t^2} \left(\frac{\delta_P}{\min(1, \delta_\Phi)^{3t}} \right)^{t|E|}. \end{aligned}$$

□

4. CYCLOTOMIC POLYNOMIALS

In order to apply Proposition 3.1 to the proof of our main Theorem 1.1, we need a lower bound for the absolute value of a cyclotomic polynomial on an appropriate subset of a finitely generated subgroup of \mathbb{C}^\times . When the generators of that subgroup do not all have absolute value one, the required estimate is easy to derive. The reader who wants a proof of Theorem 1.1 under this simplifying assumption can skip this section and go directly to the last proposition of the next section where a suitable estimate is proved.

For the rest of this section, we fix a positive integer m and non-zero complex numbers ξ_1, \dots, ξ_m . For each m -tuple of integers $\mathbf{i} = (i_1, \dots, i_m)$, we write for shortness $\underline{\xi}^{\mathbf{i}} = \xi_1^{i_1} \cdots \xi_m^{i_m}$, and we define $\|\mathbf{i}\| = \max\{|i_1|, \dots, |i_m|\}$ to be the maximum norm of \mathbf{i} . Our goal is to prove the following result dealing with values of cyclotomic polynomials at the points $\underline{\xi}^{\mathbf{i}}$.

Proposition 4.1. *Let $d, N \in \mathbb{N}^*$ and $\delta \in \mathbb{R}$ with*

$$(14) \quad 0 < \delta \leq (8md^4N)^{-2md},$$

and let $\Phi \in \mathbb{Z}[T]$ be a cyclotomic polynomial of degree $\leq d$. Then, there exist relatively prime positive integers a_1, \dots, a_m, D with $D \leq (2md^2N)^m$ such that, upon defining

$$L(i_1, \dots, i_m) = a_1 i_1 + \cdots + a_m i_m$$

for each $(i_1, \dots, i_m) \in \mathbb{Z}^m$, at least one of the following conditions holds:

- 1) *There exists a proper subspace U of \mathbb{Q}^m such that we have $|\Phi(\underline{\xi}^{\mathbf{i}})| \geq \delta$ for any point $\mathbf{i} \in \mathbb{Z}^m$ with $\mathbf{i} \notin U$, $\|\mathbf{i}\| \leq N$ and $\gcd(L(\mathbf{i}), D) = 1$.*
- 2) *There exists a root Z of Φ which is a root of unity of order exactly D such that, upon denoting by G the multiplicity of Z as a root of Φ , we have $|\underline{\xi}^{\mathbf{i}} - Z^{L(\mathbf{i})}|^G \leq \delta^{1/2}$ for each $\mathbf{i} \in \mathbb{Z}^m$ with $\|\mathbf{i}\| \leq N$.*

When the condition 2) does not hold, the condition 1) necessarily holds and provides the kind of estimate that we are looking for. This happens for example when ξ_1, \dots, ξ_m do not all have absolute value one and when N is sufficiently large in terms of ξ_1, \dots, ξ_m , because under the condition 2) we find, for each $j = 1, \dots, m$,

$$||\xi_j| - 1| \leq |\xi_j - Z^{a_j}| \leq \delta^{1/(2G)} \leq \delta^{1/(2d)} \leq (8md^4N)^{-m}.$$

In the next section we carry an independent analysis of this situation (see Proposition 5.3). We also show that the condition 2) cannot hold for N sufficiently large when ξ_1, \dots, ξ_m are as in the statement of our main theorem, with $m \geq 2$.

Before going into the proof of Proposition 4.1, we also note that the conditions 1) and 2) are almost mutually exclusive in the following sense. Suppose that the condition 2) holds, and let \mathbf{i} be any point of \mathbb{Z}^m satisfying $\|\mathbf{i}\| \leq N$ and $\gcd(L(\mathbf{i}), D) = 1$. Then, we have

$|\underline{\xi}^i| \leq 1 + \delta^{1/(2G)} \leq 2$, and $Z^{L(i)}$ is a conjugate of Z over \mathbb{Q} . So the latter is also a root of Φ of multiplicity G . Upon writing $\Phi(T) = \Psi(T)(T - Z^{L(i)})^G$ with $\Psi \in \mathbb{C}[T]$, we find that $|\Psi(\underline{\xi}^i)| \leq (|\underline{\xi}^i| + 1)^d \leq 3^d$ (since Ψ is monic of degree at most d with all its roots of absolute value one), and thus $|\Phi(\underline{\xi}^i)| \leq 3^d \delta^{1/2}$.

The proof of Proposition 4.1 requires several lemmas about cyclotomic polynomials and their roots. The first three of them are quite general.

Lemma 4.2. *Let $d \in \mathbb{N}^*$, let $\Phi \in \mathbb{Z}[T]$ be a cyclotomic polynomial of degree at most d , and let ζ be a root of Φ . Denote by ℓ the order of ζ as a root of unity, and by g its multiplicity as a root of Φ . Then, we have*

$$(15) \quad \ell \leq \frac{2d \log_2(2d)}{g} \leq 2d^2,$$

where \log_2 stands for the logarithm in base 2.

Proof. The theory of cyclotomic fields gives $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(\ell)$ where ϕ denotes Euler's totient function. Since ζ is a root of Φ of multiplicity g , this implies that $g\phi(\ell) \leq d$. Putting $k = \omega(\ell) + 1$ where $\omega(\ell)$ denotes the number of distinct prime factors of ℓ , we have $k \geq 1$,

$$\phi(\ell) = \ell \prod_{p|\ell} \left(1 - \frac{1}{p}\right) \geq \ell \prod_{i=2}^k \left(1 - \frac{1}{i}\right) = \frac{\ell}{k} \quad \text{and} \quad \ell \geq \prod_{p|\ell} p \geq k!.$$

Since $k! \geq k^2/2$, this gives $k \leq \sqrt{2\ell}$, so $\phi(\ell) \geq \sqrt{\ell/2}$, and thus $\ell \leq 2\phi(\ell)^2$. Since $k! \geq 2^{k-1}$, we also find $k \leq 1 + \log_2(\ell)$ which combined with the previous upper bound for ℓ gives $k \leq 2 \log_2(2\phi(\ell))$. Since $\phi(\ell) \leq d/g \leq d$, we conclude that $k \leq 2 \log_2(2d)$ and consequently $\ell \leq k\phi(\ell) \leq 2(d/g) \log_2(2d)$. \square

For roots of unity, Liouville's inequality takes a very simple form:

Lemma 4.3. *Let ζ_1 and ζ_2 be two distinct roots of unity with respective orders ℓ_1 and ℓ_2 . Then, we have*

$$|\zeta_1 - \zeta_2| \geq \frac{4}{\ell_1 \ell_2}.$$

Proof. For $j = 1, 2$, write $\zeta_j = \exp(2\pi r_j \sqrt{-1})$ where r_j is a rational number with denominator ℓ_j . Upon subtracting from r_1 a suitable integer, we can arrange that $|r_1 - r_2| \leq 1/2$. Since $|\exp(t\sqrt{-1}) - 1| \geq 2|t|/\pi$ for any real number t with $|t| \leq \pi$, we deduce that

$$|\zeta_1 - \zeta_2| = |\exp(2\pi(r_1 - r_2)\sqrt{-1}) - 1| \geq 4|r_1 - r_2|.$$

Since $r_1 - r_2$ is a non-zero rational number with denominator dividing $\ell_1 \ell_2$, we also have $|r_1 - r_2| \geq (\ell_1 \ell_2)^{-1}$ and the conclusion follows. \square

Lemma 4.4. *Let $d \in \mathbb{N}^*$ and let $\Phi \in \mathbb{Z}[T]$ be a cyclotomic polynomial of degree at most d . For any $\xi \in \mathbb{C}$, there exists a root ζ of Φ with*

$$(16) \quad |\xi - \zeta|^g \leq (2d^4)^d |\Phi(\xi)|,$$

where g denotes the multiplicity of ζ as a root of Φ .

Proof. Let ζ be a root of Φ which is closest to ξ , and let g be its multiplicity. Since Φ is monic, we can write $\Phi(T) = (T - \zeta_1) \cdots (T - \zeta_s)$ where $s \leq d$ is the degree of Φ and where ζ_1, \dots, ζ_s are roots of unity with $\zeta_1 = \cdots = \zeta_g = \zeta$. By Lemma 4.2, each ζ_j has order at most $2d^2$. Thus, for $j = g + 1, \dots, s$, Lemma 4.3 gives $|\zeta - \zeta_j| \geq d^{-4}$. For the same values of j we also have $|\zeta - \zeta_j| \leq |\xi - \zeta| + |\xi - \zeta_j| \leq 2|\xi - \zeta|$ by virtue of the choice of ζ , and so $|\xi - \zeta_j| \geq (2d^4)^{-1}$. This gives $|\Phi(\xi)| \geq |\xi - \zeta|^g (2d^4)^{g-s} \geq |\xi - \zeta|^g (2d^4)^{-d}$. \square

The last lemma is more technical and provides the key to the proof of Proposition 4.1.

Lemma 4.5. *Let $\ell, N \in \mathbb{N}^*$ and $\rho \in \mathbb{R}$ with $0 < \rho \leq (1/2)(mN)^{-m}$. Suppose that there exist linearly independent points $\mathbf{i}^{(1)}, \dots, \mathbf{i}^{(m)}$ of \mathbb{Z}^m of norm at most N , and roots of unity ζ_1, \dots, ζ_m of order at most ℓ such that $|\underline{\xi}^{\mathbf{i}^{(k)}} - \zeta_k| \leq \rho$ for $k = 1, \dots, m$. Then, there exist an integer D with $1 \leq D \leq (\ell m N)^m$, a root of unity Z of order D , and non-zero integers a_1, \dots, a_m with $\gcd(a_1, \dots, a_m, D) = 1$ such that, for each $\mathbf{i} = (i_1, \dots, i_m) \in \mathbb{Z}^m$ with norm $\|\mathbf{i}\| \leq N$, we have*

$$(17) \quad |\underline{\xi}^{\mathbf{i}} - Z^{a_1 i_1 + \dots + a_m i_m}| \leq 4(mN)^m \rho.$$

Proof. For $k = 1, \dots, m$, we can write $\underline{\xi}^{\mathbf{i}^{(k)}} = \zeta_k(1 + \rho_k)$ for a complex number ρ_k with $|\rho_k| \leq \rho$. Put $\rho'_k = \log(1 + \rho_k) = -\sum_{j=1}^{\infty} (-\rho_k)^j / j$. Since $|\rho_k| \leq 1/2$, we find $|\rho'_k| \leq 2|\rho_k|$, and so

$$(18) \quad \underline{\xi}^{\mathbf{i}^{(k)}} = \zeta_k \exp(\rho'_k) \quad \text{with} \quad |\rho'_k| \leq 2\rho.$$

Let M be the square $m \times m$ matrix whose rows are $\mathbf{i}^{(1)}, \dots, \mathbf{i}^{(m)}$. For $j = 1, \dots, m$, let (b_{j1}, \dots, b_{jm}) denote the j -th row of the adjoint of M , and let \mathbf{e}_j denote the j -th row of the $m \times m$ identity matrix. Since $\det(M)\mathbf{e}_j = b_{j1}\mathbf{i}^{(1)} + \dots + b_{jm}\mathbf{i}^{(m)}$, we find by (18)

$$(19) \quad \xi_j^{\det(M)} = \zeta_1^{b_{j1}} \cdots \zeta_m^{b_{jm}} \exp\left(\sum_{k=1}^m b_{jk} \rho'_k\right).$$

Since $|b_{jk}| \leq (m-1)!N^{m-1}$ for $k = 1, \dots, m$ and since $\det(M)$ is a non-zero integer, we deduce from (18) and (19) that

$$(20) \quad \xi_j = Z_j \exp(\rho''_j) \quad \text{with} \quad Z_j^{\det(M)} = \zeta_1^{b_{j1}} \cdots \zeta_m^{b_{jm}} \quad \text{and} \quad |\rho''_j| \leq 2m!N^{m-1}\rho.$$

Let Z be a generator of the subgroup of $\mathbb{C}_{\text{tor}}^\times$ spanned by Z_1, \dots, Z_m , and let D be the order of Z . Since $Z^{\det(M)}$ belongs to the subgroup spanned by ζ_1, \dots, ζ_m and since the latter have order at most ℓ , the order D of Z is at most $\ell^m |\det(M)| \leq (\ell m N)^m$. For $j = 1, \dots, m$, we

choose an integer $a_j \geq 1$ such that $Z_j = Z^{a_j}$. Then, because of the choice of Z , we have $\gcd(a_1, \dots, a_m, D) = 1$, and for each $\mathbf{i} = (i_1, \dots, i_m) \in \mathbb{Z}^m$ with $\|\mathbf{i}\| \leq N$ we find by (20)

$$(21) \quad \underline{\xi}^{\mathbf{i}} = Z^{a_1 i_1 + \dots + a_m i_m} \exp(\rho_{\mathbf{i}}''') \quad \text{with} \quad |\rho_{\mathbf{i}}'''| \leq (mN)(2m!N^{m-1}\rho) \leq 2(mN)^m \rho.$$

Since $|\rho_{\mathbf{i}}'''| \leq 1$, we also have $|\exp(\rho_{\mathbf{i}}''') - 1| \leq 2|\rho_{\mathbf{i}}'''|$ and so (17) follows. \square

Proof of Proposition 4.1. Let I_N denote the set of points $\mathbf{i} \in \mathbb{Z}^m$ with $\|\mathbf{i}\| \leq N$, and let $I_{N,\Phi}$ denote the set of points $\mathbf{i} \in I_N$ such that $|\Phi(\underline{\xi}^{\mathbf{i}})| < \delta$. If $I_{N,\Phi}$ is contained in a proper subspace U of \mathbb{Q}^m , we are done. Assume the contrary. Then, since $I_{N,\Phi}$ is a finite set, there exists a smallest positive real number ρ for which it contains m linearly independent points $\mathbf{i}^{(1)}, \dots, \mathbf{i}^{(m)}$ with the property that each of the complex numbers $\underline{\xi}^{\mathbf{i}^{(1)}}, \dots, \underline{\xi}^{\mathbf{i}^{(m)}}$ is at a distance $\leq \rho$ from a zero of Φ . Lemma 4.4 shows that, for each $\mathbf{i} \in I_{N,\Phi}$, there exists a root ζ of Φ with

$$(22) \quad |\underline{\xi}^{\mathbf{i}} - \zeta|^g \leq (2d^4)^d \delta$$

where g denotes the multiplicity of ζ . Since $g \leq d$, this implies that $\rho \leq 2d^4 \delta^{1/d}$. Since the hypothesis (14) gives $2d^4 \delta^{1/d} \leq (2mN)^{-m}$ and since, by Lemma 4.2, any root ζ of Φ has order $\leq 2d^2$, Lemma 4.5 provides us with relatively prime positive integers a_1, \dots, a_m, D with $D \leq (2d^2 mN)^m$, and a root of unity Z of order D , such that for each $\mathbf{i} = (i_1, \dots, i_m) \in I_N$, we have

$$(23) \quad |\underline{\xi}^{\mathbf{i}} - Z^{L(\mathbf{i})}| \leq 4(mN)^m \rho, \quad \text{where } L(\mathbf{i}) = a_1 i_1 + \dots + a_m i_m.$$

If we choose $\mathbf{i} \in I_{N,\Phi}$ and if ζ is a root of Φ satisfying (22), this gives

$$(24) \quad |\zeta - Z^{L(\mathbf{i})}| \leq (1 + 4(mN)^m) 2d^4 \delta^{1/d}.$$

As ζ and $Z^{L(\mathbf{i})}$ are roots of unity of order at most $2d^2$ and D respectively and since by (14) the right hand side of (24) is at most $4d^4(4mN)^m(8md^4N)^{-2m} < 4D^{-1}(2d^2)^{-1}$, we conclude, by Lemma 4.3, that both roots of unity are equal. Therefore, $Z^{L(\mathbf{i})} = \zeta$ is a root of Φ when $\mathbf{i} \in I_{N,\Phi}$.

Finally, let $I_{N,\Phi,D}$ denote the set of points $\mathbf{i} \in I_{N,\Phi}$ with $\gcd(L(\mathbf{i}), D) = 1$. Again, if this set is contained in a proper subspace of \mathbb{Q}^m , the first condition of the proposition holds. Suppose on the contrary that $I_{N,\Phi,D}$ contains m linearly independent points. For each $\mathbf{i} \in I_{N,\Phi,D}$, the root of unity $Z^{L(\mathbf{i})}$ is a conjugate of Z over \mathbb{Q} , so it is a root of Φ of the same multiplicity G as Z , and the inequality (22) gives $|\underline{\xi}^{\mathbf{i}} - Z^{L(\mathbf{i})}|^G \leq (2d^4)^d \delta$. As $I_{N,\Phi,D}$ contains m linearly independent points, this means that $\rho^G \leq (2d^4)^d \delta$. By (23) and the fact that $G \leq d$, we conclude that, for each $\mathbf{i} \in I_N$, we have

$$|\underline{\xi}^{\mathbf{i}} - Z^{L(\mathbf{i})}|^G \leq (4(mN)^m \rho)^G \leq (4mN)^{md} (2d^4)^d \delta \leq \delta^{1/2}.$$

\square

5. AVOIDING CYCLOTOMIC FACTORS IN RANK AT LEAST TWO

In this section, we consider two instances where only the first alternative in Proposition 4.1 holds. As observed in the preceding section, the simplest case is when ξ_1, \dots, ξ_m do not all have absolute value one. The reader who wants to restrict to this situation can go directly to Proposition 5.3, where a short independent proof is given, and omit the rest of the section. The second case is when ξ_1, \dots, ξ_m are multiplicatively independent with $m \geq 2$, and generate over \mathbb{Q} a field of transcendence degree one. To show that the latter condition is sufficient, we first establish the following measure of simultaneous approximation by roots of unity, where ϕ stands for the Euler totient function.

Proposition 5.1. *Let $m \geq 2$ be an integer, and let $\xi_1, \dots, \xi_m \in \mathbb{C}^\times$ be multiplicatively independent non-zero complex numbers which generate over \mathbb{Q} a field of transcendence degree one. For any choice of positive integers a_1, \dots, a_m, D and for any root of unity $Z \in \mathbb{C}_{\text{tor}}^\times$ of order D , we have*

$$(25) \quad \max_{1 \leq j \leq m} |\xi_j - Z^{a_j}| > c^{\phi(D)}$$

where c is a constant depending only on ξ_1, \dots, ξ_m with $0 < c \leq 1$.

In the proof below as well as in the rest of the section, we use the same notation as in Section 4. Namely, we denote by $\|\mathbf{i}\|$ the maximum norm of an integer point $\mathbf{i} = (i_1, \dots, i_m) \in \mathbb{Z}^m$, and we define $\xi_{\mathbf{i}} = \xi_1^{i_1} \cdots \xi_m^{i_m}$.

Proof. The field $R = \mathbb{Q}(\xi_1, \dots, \xi_m)$ is a field of functions in one variable over \mathbb{Q} (see Chapter 1 of [2]). Let K denote its field of constants and, for $j = 1, \dots, m$, let \mathfrak{b}_j denote the divisor of poles of ξ_j . Let J be the ideal of polynomials of $\mathbb{Q}[T_1, \dots, T_m]$ which vanish at the point (ξ_1, \dots, ξ_m) , and let P_1, \dots, P_s be a system of generators of this ideal, chosen in $\mathbb{Z}[T_1, \dots, T_m]$. Define

$$c_1 = \max_{1 \leq k \leq s} \left(L(P_k) \max_{1 \leq j \leq m} (1 + |\xi_j|)^{\deg(P_k)} \right) \quad \text{and} \quad c_2 = [K : \mathbb{Q}] \sum_{j=1}^m \deg(\mathfrak{b}_j),$$

and choose a real number c with $0 < c < c_1^{-1}$ such that (25) holds whenever $D \leq (3c_2)^6$ (this involves a finite number of inequalities). We claim that, for such a value of c , the estimate (25) holds in general.

To prove this, suppose on the contrary that there exist positive integers a_1, \dots, a_m, D and a root of unity Z of order D which satisfy

$$\max_{1 \leq j \leq m} |\xi_j - Z^{a_j}| \leq c^{\phi(D)}.$$

Upon replacing a_1, \dots, a_m, D and Z respectively by $a_1/a, \dots, a_m/a, D/a$ and Z^a where $a = \gcd(a_1, \dots, a_m, D)$, we may assume without loss of generality that a_1, \dots, a_m, D are

relatively prime. For each $k = 1, \dots, s$, the norm of $P_k(Z^{a_1}, \dots, Z^{a_m})$ from $\mathbb{Q}(Z)$ to \mathbb{Q} is an integer given by

$$N_{\mathbb{Q}(Z)/\mathbb{Q}}(P_k(Z^{a_1}, \dots, Z^{a_m})) = \prod_{\substack{1 \leq j \leq D \\ \gcd(j, D)=1}} P_k(Z^{ja_1}, \dots, Z^{ja_m}).$$

Since $|P_k(Z^{a_1}, \dots, Z^{a_m})| = |P_k(\xi_1, \dots, \xi_m) - P_k(Z^{a_1}, \dots, Z^{a_m})| \leq c_1 \max_{1 \leq j \leq m} |\xi_j - Z^{a_j}|$, and since $|P_k(Z^{ja_1}, \dots, Z^{ja_m})| \leq L(P_k) \leq c_1$ for each integer j , we deduce that

$$|N_{\mathbb{Q}(Z)/\mathbb{Q}}(P_k(Z^{a_1}, \dots, Z^{a_m}))| \leq c_1^{\phi(D)} \max_{1 \leq j \leq m} |\xi_j - Z^{a_j}| \leq (c_1 c)^{\phi(D)} < 1.$$

Thus the norm of $P_k(Z^{a_1}, \dots, Z^{a_m})$ is 0 and so we have $P_k(Z^{a_1}, \dots, Z^{a_m}) = 0$ for $k = 1, \dots, s$. According to [2, Ch. 1, §4, Cor. 1], this implies the existence of a place \mathfrak{p} of R which is a common zero of $\xi_1 - Z^{a_1}, \dots, \xi_m - Z^{a_m}$. The residue field of this place contains $\mathbb{Q}[Z^{a_1}, \dots, Z^{a_m}]$ which is simply $\mathbb{Q}(Z)$ since $\gcd(a_1, \dots, a_m, D) = 1$. Thus, we have

$$(26) \quad [K : \mathbb{Q}] \deg(\mathfrak{p}) \geq [\mathbb{Q}(Z) : \mathbb{Q}] = \phi(D).$$

Define $L(\mathbf{i}) = a_1 i_1 + \dots + a_m i_m$ for each $\mathbf{i} = (i_1, \dots, i_m) \in \mathbb{Z}^m$, and choose any non-zero point $\mathbf{i} \in \mathbb{Z}^m$ such that $L(\mathbf{i}) \equiv 0 \pmod{D}$. Since ξ_1, \dots, ξ_m are multiplicatively independent, the difference $\eta = \underline{\xi}^{\mathbf{i}} - 1$ is a non-zero element of R . Let \mathfrak{a} denote its divisor of zeros, and \mathfrak{b} its divisor of poles. Then \mathfrak{a} and \mathfrak{b} have the same degree. Similarly, for each $j = 1, \dots, m$ the divisor of zeros \mathfrak{a}_j of ξ_j has the same degree as its divisor of poles \mathfrak{b}_j . Since \mathfrak{b} is also the divisor of poles of $\underline{\xi}^{\mathbf{i}} = \xi_1^{i_1} \cdots \xi_m^{i_m}$, we deduce that

$$\deg(\mathfrak{b}) \leq \|\mathbf{i}\| \sum_{j=1}^m \deg(\mathfrak{b}_j).$$

On the other hand, since $Z^{L(\mathbf{i})} = 1$, the place \mathfrak{p} is a zero of η and so we have $\deg(\mathfrak{a}) \geq \deg(\mathfrak{p})$. Combining this with (26) and the above inequality, we conclude that

$$\phi(D) \leq [K : \mathbb{Q}] \deg(\mathfrak{p}) \leq [K : \mathbb{Q}] \deg(\mathfrak{a}) = [K : \mathbb{Q}] \deg(\mathfrak{b}) \leq c_2 \|\mathbf{i}\|.$$

This observation implies that the function $f: \mathbb{Z}^m \rightarrow \mathbb{Z}/D\mathbb{Z}$ given by $f(\mathbf{i}) = L(\mathbf{i}) + D\mathbb{Z}$ ($\mathbf{i} \in \mathbb{Z}^m$) is injective on the set of points $\mathbf{i} \in \mathbb{N}^m$ with $\|\mathbf{i}\| < c_2^{-1} \phi(D)$, and therefore we have

$$(27) \quad D \geq (c_2^{-1} \phi(D))^m \geq (c_2^{-1} \phi(D))^2.$$

On the other hand, since Z is a root of a cyclotomic polynomial of degree $\phi(D)$, Lemma 4.2 gives $D \leq 2\phi(D) \log_2(2\phi(D)) \leq 3\phi(D) \log(2\phi(D))$. Since $\log(x) \leq \sqrt{x}$ for any positive real number x , this leads to $D \leq (3\phi(D))^{3/2}$ which combined with (27) gives $D \leq (3c_2)^6$. This is a contradiction since we chose c so that (25) holds for such a value of D . \square

Combining the above result with Proposition 4.1, we obtain:

Corollary 5.2. *Let m, ξ_1, \dots, ξ_m and c be as in the statement of Proposition 5.1. Let $d, N \in \mathbb{N}^*$ and $\delta \in \mathbb{R}$ with*

$$(28) \quad 0 < \delta \leq \min\{(8md^4N)^{-m}, c\}^{2d},$$

and let $\Phi \in \mathbb{Z}[T]$ be a cyclotomic polynomial of degree $\leq d$. Then, there exist relatively prime positive integers a_1, \dots, a_m, D with $D \leq (2md^2N)^m$ and a proper subspace U of \mathbb{Q}^m such that we have $|\Phi(\underline{\xi}^{\mathbf{i}})| \geq \delta$ for any point $\mathbf{i} = (i_1, \dots, i_m) \in \mathbb{Z}^m \setminus U$ with $\|\mathbf{i}\| \leq N$ and $\gcd(a_1i_1 + \dots + a_mi_m, D) = 1$.

Proof. Let Z be a root of Φ , let D denote its order as a root of unity, and let G denote its multiplicity as a root of Φ . Since $d \geq \deg(\Phi) \geq G\phi(D)$, Proposition 5.1 gives

$$\max_{1 \leq j \leq m} |\xi_j - Z^{a_j}|^G > c^{G\phi(D)} \geq c^d \geq \delta^{1/2}$$

for any choice of positive integers a_1, \dots, a_m . The conclusion follows by Proposition 4.1. \square

The next result provides a substitute to Corollary 5.2 when ξ_1, \dots, ξ_m do not all have absolute value one.

Proposition 5.3. *Let $m \geq 2$ be an integer, let $\xi_1, \dots, \xi_m \in \mathbb{C}^\times$ be non-zero complex numbers not all of absolute value 1, and let N be a positive integer. If N is sufficiently large, there exists a proper subspace U of \mathbb{Q}^m such that we have $|\Phi(\underline{\xi}^{\mathbf{i}})| \geq (8mN)^{-md}$ for each positive integer d , each cyclotomic polynomial $\Phi \in \mathbb{Z}[T]$ of degree $\leq d$, and each point $\mathbf{i} \in \mathbb{Z}^m \setminus U$ with $\|\mathbf{i}\| \leq N$.*

Proof. Write $\xi_j = \exp(u_j + v_j\sqrt{-1})$ with $u_j, v_j \in \mathbb{R}$, for $j = 1, \dots, m$. Then, u_1, \dots, u_m are not all zero, and by a result of Dirichlet (see for example [8, Ch. II, Thm 1A]), there exist integers a_1, \dots, a_m and b satisfying $1 \leq b \leq (2mN)^m$ and $|bu_j - a_j| \leq (2mN)^{-1}$ for $j = 1, \dots, m$. If N is large enough, the integers a_1, \dots, a_m are not all zero, and so the equation $a_1x_1 + \dots + a_mx_m = 0$ defines a proper subspace U of \mathbb{Q}^m . For any $\mathbf{i} = (i_1, \dots, i_m) \in \mathbb{Z}^m \setminus U$ with $\|\mathbf{i}\| \leq N$, we have $|a_1i_1 + \dots + a_mi_m| \geq 1$ and thus

$$\begin{aligned} |u_1i_1 + \dots + u_mi_m| &\geq \frac{1}{b} \left| \sum_{j=1}^m a_j i_j \right| - \frac{1}{b} \sum_{j=1}^m |bu_j - a_j| |i_j| \\ &\geq \frac{1}{b} - \frac{1}{b} m(2mN)^{-1} N = \frac{1}{2b} \geq (4mN)^{-m}. \end{aligned}$$

Since $|\exp(x) - 1| \geq |x|/2$ for each $x \in \mathbb{R}$ with $|x| \leq 1/2$, we deduce that for the same choice of \mathbf{i} and any root of unity $\zeta \in \mathbb{C}_{\text{tor}}^\times$, we have

$$|\underline{\xi}^{\mathbf{i}} - \zeta| \geq \left| |\underline{\xi}^{\mathbf{i}}| - 1 \right| = |\exp(u_1i_1 + \dots + u_mi_m) - 1| \geq 1 - \exp(-(4mN)^{-m}) \geq (8mN)^{-m}.$$

Consequently, for any positive integer d and any cyclotomic polynomial $\Phi \in \mathbb{Z}[T]$ of degree $\leq d$, we get $|\Phi(\underline{\xi}^{\mathbf{i}})| \geq (8mN)^{-md}$. \square

6. ESTIMATES FOR AN INTERSECTION

Throughout this section, we fix an abelian group \mathbb{G} with its group law denoted multiplicatively, and we fix a finite set of prime numbers A with cardinality at least 2. We denote by \mathbb{G}_{tor} the torsion subgroup of \mathbb{G} . For each subset E of \mathbb{G} , we define

$$\mathcal{O}(E) = \{x^p; x \in E, p \in A\}.$$

For a singleton $\{x\}$, we simply write $\mathcal{O}(x)$ to denote $\mathcal{O}(\{x\})$. Then, for any subset E of \mathbb{G} , we have $\mathcal{O}(E) = \cup_{x \in E} \mathcal{O}(x)$. For each $x \in \mathbb{G}$ and each integer $k \geq 1$, we also define $C_k(x)$ to be the set of all elements y of \mathbb{G} which satisfy a relation of the form

$$(29) \quad x^{p_1 \cdots p_k} = y^{q_1 \cdots q_k},$$

for a choice of prime numbers $p_1, \dots, p_k, q_1, \dots, q_k$ in A (not necessarily distinct). We also define $C_0(x) = \{x\}$. With this notation, the main result of this section reads as follows:

Proposition 6.1. *Let E and F be finite non-empty subsets of \mathbb{G} with $\mathcal{O}(E) \subseteq F$ and $E \cap \mathbb{G}_{\text{tor}} = \emptyset$. Suppose that*

$$(30) \quad |F| \leq \frac{1}{2^{\ell+1}(\ell+1)!} \binom{|A|}{\ell+2}$$

for some integer ℓ with $0 \leq \ell \leq |A| - 2$. Then, there exist an integer $r \geq 1$, a sequence of points x_1, \dots, x_r of E , and partitions $E = E_1 \amalg \cdots \amalg E_r$ and $F = F_1 \amalg \cdots \amalg F_r \amalg F_{r+1}$ of E and F which, for $i = 1, \dots, r$, satisfy

$$a) E_i \subseteq C_\ell(x_i), \quad b) F_i \subseteq \mathcal{O}(E_i), \quad c) |F_i| \geq \frac{|A| - \ell}{2(\ell+1)} |E_i|.$$

This result can be viewed as a generalization of Proposition 6.2 of [7] (see the remark at the end of this section for more details on how to derive the latter from the former). Its proof will follow the same general pattern, although additional difficulties come into play due to the fact that \mathbb{G} may contain non-trivial torsion elements. To deal with these, we use several additional notions.

First of all, we say that two elements x and y of \mathbb{G} are A -equivalent and we write $x \sim_A y$ if there exist finite sequences (p_1, \dots, p_k) and (q_1, \dots, q_ℓ) of elements of A such that

$$(31) \quad x^{p_1 \cdots p_k} = y^{q_1 \cdots q_\ell}.$$

This defines an equivalence relation on \mathbb{G} . In view of the preceding definitions, for any $x \in \mathbb{G}$ and any integer $k \geq 0$, the equivalence class of x contains $C_k(x)$.

Fix a non-torsion element x of \mathbb{G} and a point y in the same equivalence class. Then, y is also a non-torsion element of G . Moreover, if $\langle x \rangle$ denotes the subgroup of \mathbb{G} generated by x , then the set of integers i such that $y^i \in \langle x \rangle$ is a non-trivial subgroup of \mathbb{Z} . We define $\text{den}_x(y)$ to be the positive generator n of this group. Then, since x is non-torsion, there exists a unique integer m such that $y^n = x^m$, and we define $\text{num}_x(y) = m$. Note that these

integers m and n may not be relatively prime, and therefore the fraction m/n may not be in reduced form. However, the following lemma shows useful properties for these notions of logarithmic “numerator” and “denominator” of y with respect to x .

Lemma 6.2. *Let x and y be non-torsion elements of \mathbb{G} in the same equivalence class. Put $n = \text{den}_x(y)$ and $m = \text{num}_x(y)$, and choose elements $p_1, \dots, p_k, q_1, \dots, q_\ell$ of A such that (31) holds. Then, m (resp. n) is a positive divisor of $p_1 \cdots p_k$ (resp. $q_1 \cdots q_\ell$), and we have*

$$(32) \quad \frac{m}{n} = \frac{p_1 \cdots p_k}{q_1 \cdots q_\ell}.$$

Moreover, if q is an element of A not dividing n , then the point $z = y^q$ satisfies $\text{den}_x(z) = n$ and $\text{num}_x(z) = qm$.

Proof. Since $x \notin \mathbb{G}_{\text{tor}}$, the equality (31) combined with $y^n = x^m$ leads to (32). Moreover, as (31) gives $y^{q_1 \cdots q_\ell} \in \langle x \rangle$, it follows from the definition of $\text{den}_x(y)$ that n is a positive divisor of $q_1 \cdots q_\ell$. Then, since all the elements of A are positive, we deduce from (32) that m is a positive divisor of $p_1 \cdots p_k$. This proves the first part of the lemma.

For the second part, fix a prime number $q \in A$ not dividing n . Put $z = y^q$, $n' = \text{den}_x(z)$ and $m' = \text{num}_x(z)$. Since $z^n = y^{qn} = x^{qm} \in \langle x \rangle$, it follows, by definition of n' , that n' divides n . Moreover, since $y^{qn'} = z^{n'} = x^{m'} \in \langle x \rangle$, it also follows from the definition of n that n divides qn' . Since, by hypothesis, q and n are relatively prime, and since n and n' are positive, these two divisibility relations imply that $n = n'$. Then, since $x \notin \mathbb{G}_{\text{tor}}$, the equality $x^{m'} = z^n = x^{qm}$ implies that $m' = qm$. \square

For any integer $k \geq 0$, any non-torsion point x of \mathbb{G} and any subset E of \mathbb{G} , we define

$$C_k(x, E) = C_k(x) \cap E \quad \text{and} \quad D_k(x, E) = \mathcal{O}(C_k(x, E)).$$

With this notation, the first part of Lemma 6.2 shows that, for each $y \in C_k(x, E)$ and each $z \in D_k(x, E)$, the integers $\text{den}_x(y)$, $\text{num}_x(y)$ and $\text{den}_x(z)$ are products of at most k elements of A , while $\text{num}_x(z)$ is a product of at most $k + 1$ elements of A , counting multiplicities. We also note that if a subset F of \mathbb{G} contains $\mathcal{O}(E)$, then it contains $D_k(x, E)$. The next lemma compares the sizes of $C_k(x, E)$ and $D_k(x, E)$.

Lemma 6.3. *Let E be a finite subset of \mathbb{G} , let $k \geq 0$ be an integer, and let $x \in \mathbb{G}$ with $x \notin \mathbb{G}_{\text{tor}}$. Then, we have*

$$|D_k(x, E)| \geq \frac{|A| - k}{k + 1} |C_k(x, E)|.$$

Proof. Put $C = C_k(x, E)$ and $D = \mathcal{O}(C)$, so that $D = D_k(x, E)$. We denote by N the set of all pairs $(y, q) \in C \times A$ such that q divides $\text{den}_x(y)$, and we put $P = (C \times A) \setminus N$. Then, since N and P form a partition of $C \times A$, we have

$$(33) \quad |N| + |P| = |C| |A|.$$

For any given $y \in C$, the integer $\text{den}_x(y)$ is a product of at most k prime numbers (including multiplicities). Therefore there are at most k distinct elements q of A such that $(y, q) \in N$. This being true for each $y \in C$, we deduce that

$$(34) \quad |N| \leq k|C|.$$

Consider the surjective map $\varphi: C \times A \rightarrow D$ given by $\varphi(y, q) = y^q$ for each $(y, q) \in C \times A$. We claim that, for each $z \in D$, we have $|\varphi^{-1}(z) \cap P| \leq k + 1$. If we admit this result, then we find

$$|P| = |\varphi^{-1}(D) \cap P| \leq (k + 1)|D|,$$

and by combining this estimate with (33) and (34), we deduce that

$$(k + 1)|D| \geq |P| = |A||C| - |N| \geq (|A| - k)|C|,$$

as announced.

To prove the above claim, suppose that $(y, q) \in \varphi^{-1}(z) \cap P$ for some fixed $z \in D$. Put $n = \text{den}_x(y)$ and $m = \text{num}_x(y)$. By hypothesis, we have $y^q = z$ and q is prime to n . According to Lemma 6.2, this implies that $\text{den}_x(z) = n$ and $\text{num}_x(z) = qm$. So, n is known (it depends only on x and z) and q is a prime divisor of $\text{num}_x(z)$. Moreover, since $z \in D$, the integer $\text{num}_x(z)$ is a product of at most $k + 1$ prime numbers of A . So, this leaves at most $k + 1$ possibilities for q . Once q is known, the relation $\text{num}_x(z) = qm$ uniquely determines m , and the conditions $y^q = z$ and $y^n = x^m$ in turn determine y : since q is prime to n , we can write $1 = aq + bn$ with $a, b \in \mathbb{Z}$ and then we find $y = z^a x^{bm}$. Thus $\varphi^{-1}(z)$ contains at most $k + 1$ elements (y, q) of P . \square

Lemma 6.4. *Let E be a finite subset of \mathbb{G} , let $k \geq 0$ be an integer, and let $x \in \mathbb{G}$ with $x \notin \mathbb{G}_{\text{tor}}$. Then, we have*

$$|D_k(x, E) \cap \mathcal{O}(E \setminus C_k(x, E))| \leq (k + 1)|C_{k+1}(x, E)|.$$

Proof. It suffices to show that, for any $y \in E \setminus C_k(x, E)$ such that $D_k(x, E) \cap \mathcal{O}(y) \neq \emptyset$, we have $y \in C_{k+1}(x, E)$ and $|D_k(x, E) \cap \mathcal{O}(y)| \leq k + 1$. Fix such a choice of y (assuming that there is one). Since $D_k(x, E) \cap \mathcal{O}(y) \neq \emptyset$, there exist $p, q \in A$ and $z \in C_k(x, E)$ such that $y^q = z^p$. Moreover, since $z \in C_k(x, E)$, there also exist $p_1, \dots, p_k, q_1, \dots, q_k \in A$ such that $z^{q_1 \cdots q_k} = x^{p_1 \cdots p_k}$. Combining these two relations, we obtain

$$(35) \quad y^{qq_1 \cdots q_k} = x^{pp_1 \cdots p_k},$$

which shows that $y \in C_{k+1}(x, E)$. Put $n = \text{den}_x(y)$ and $m = \text{num}_x(y)$. By Lemma 6.2, the equality (35) also implies that n divides $qq_1 \cdots q_k$ and that $m/n = (pp_1 \cdots p_k)/(qq_1 \cdots q_k)$. In particular, the factorizations of m and n into prime numbers have the same length: they involve the same number of elements of A , counting multiplicities. If j is this length, then the equality $y^n = x^m$ means that $y \in C_j(x, E)$. Since $y \notin C_k(x, E)$, we must have

$j > k$. It follows that $j = k + 1$ and $n = qq_1 \cdots q_k$. In particular, q is one of the prime factors of n . Since $n = \text{den}_x(y)$ has at most $k + 1$ distinct prime factors, we conclude that $|D_k(x, E) \cap \mathcal{O}(y)| \leq k + 1$. \square

Proof of Proposition 6.1. We proceed by induction on $|E|$. Fix a choice of $x \in E$. We claim that there exists an index k with $0 \leq k \leq \ell$ such that the sets $C_k = C_k(x, E)$ and $D_k = D_k(x, E)$ satisfy

$$(36) \quad |D_k \setminus \mathcal{O}(E \setminus C_k)| \geq \frac{|A| - k}{2(k + 1)} |C_k|.$$

If we admit this statement, then, for such k , the sets $E_1 = C_k$ and $F_1 = D_k \setminus \mathcal{O}(E \setminus C_k)$ fulfil the conditions a), b) and c) of Proposition 6.1 for $i = 1$ and the choice of $x_1 = x$. Put $E' = E \setminus E_1$ and $F' = F \setminus F_1$. Then, we have $E = E_1 \amalg E'$, $F = F_1 \amalg F'$ and $\mathcal{O}(E') \subseteq F'$. If $E' = \emptyset$, this proves the proposition with $r = 1$ and $F_2 = F'$. Otherwise, we may assume, by induction, that the proposition applies to E' and F' , and the conclusion follows.

To prove the above claim, suppose on the contrary that (36) does not hold for any $k = 0, 1, \dots, \ell$. Then, we have

$$|D_k| < |D_k \cap \mathcal{O}(E \setminus C_k)| + \frac{|A| - k}{2(k + 1)} |C_k| \quad (0 \leq k \leq \ell).$$

Combining this with the lower bound for $|D_k|$ provided by Lemma 6.3 and the upper bound for $|D_k \cap \mathcal{O}(E \setminus C_k)|$ provided by Lemma 6.4, we obtain

$$\frac{|A| - k}{2(k + 1)^2} |C_k| < |C_{k+1}| \quad (0 \leq k \leq \ell).$$

Since $C_0 = \{x\}$ has cardinality 1, this leads to $|C_{\ell+1}(x, E)| > (2^{\ell+1}(\ell + 1)!)^{-1} \binom{|A|}{\ell+1}$. Then, by Lemma 6.3, we obtain $|D_{\ell+1}(x, E)| > (2^{\ell+1}(\ell + 1)!)^{-1} \binom{|A|}{\ell+2}$. This contradicts (30) since $D_{\ell+1}(x, E)$ is a subset of F . \square

Remark. It is easy to translate the proposition to the case of an abelian group \mathbb{G} denoted additively. Choose \mathbb{G} to be the additive group of \mathbb{Q} . Let s be a positive integer, let $A = \{p_1, \dots, p_s\}$ be a set of s distinct prime numbers, and let T be A -equivalence class of 1 in $\mathbb{G} = \mathbb{Q}$. Then, Proposition 6.1 applied to arbitrary subsets E and F of T with $\mathcal{O}(E) \subseteq F$ translates into Proposition 6.2 of [7], upon identifying \mathbb{Z}^s with T under the map which sends a point $(i_1, \dots, i_s) \in \mathbb{Z}^s$ to the rational number $p_1^{i_1} \cdots p_s^{i_s}$.

7. ESTIMATES FOR THE GCD

We now apply the combinatorial result of the preceding section to provide estimates for the degree and height of the greatest common divisor of a family of polynomials of the form $P(T^a)$ where P is fixed and a varies among a finite set of integers A . The result that we prove below implies Theorem 1.2.

Theorem 7.1. *Let K be a number field, let $M, n \in \mathbb{N}^*$ with $M \geq 2$, let A be a non-empty set consisting of prime numbers p in the interval $M/2 \leq p \leq M$, let P be a non-zero polynomial of $K[T]$ of degree at most n with no root in $\mathbb{C}_{\text{tor}}^\times \cup \{0\}$, and let $Q \in K[T]$ be a greatest common divisor of the polynomials $P(T^a)$ with $a \in A$. Suppose that there exists an integer ℓ satisfying*

$$4 \leq 2\ell \leq |A| \quad \text{and} \quad n \leq \frac{1}{2^{\ell+1}(\ell+1)!} \binom{|A|}{\ell+2}.$$

Then, we have

$$(37) \quad \deg(Q) \leq \frac{6\ell}{|A|} \deg(P) \quad \text{and} \quad \log H(Q) \leq \frac{c}{|A|M} (M \deg(P) + \log H(P)),$$

with $c = \ell 2^{2\ell+6}$.

Proof. Suppose first that all roots of P are simple. Then, for each $a \in A$, the roots of $P(T^a)$ are also simple (since $P(0) \neq 0$), and so the roots of Q are simple. Define \mathbb{G} to be the multiplicative group \mathbb{C}^\times of \mathbb{C} , and let E and F denote respectively the sets of roots of Q and P . By hypothesis, we have $F \subset \mathbb{G} \setminus \mathbb{G}_{\text{tor}}$ and $|F| \leq n$. Moreover, for any $x \in E$ and any $a \in A$, x is a root of $P(T^a)$ and so we have $x^a \in F$. In the notation of §6, this means that $E \subset \mathbb{G} \setminus \mathbb{G}_{\text{tor}}$ and that $\mathcal{O}(E) \subseteq F$. If $E = \emptyset$, then Q is a constant and (37) holds. Otherwise, Proposition 6.1 provides us with an integer $r \geq 1$, a sequence of points x_1, \dots, x_r of E , and partitions $E = E_1 \amalg \dots \amalg E_r$ and $F = F_1 \amalg \dots \amalg F_{r+1}$ satisfying, for $i = 1, \dots, r$,

$$(38) \quad E_i \subseteq C_\ell(x_i), \quad F_i \subseteq \mathcal{O}(E_i) \quad \text{and} \quad |F_i| \geq \frac{|A| - \ell}{2(\ell+1)} |E_i| \geq \frac{|A|}{6\ell} |E_i|.$$

Summing term by term the last inequalities for $i = 1, \dots, r$, we obtain $|F| \geq |A| |E| / (6\ell)$ and so

$$(39) \quad \deg(Q) = |E| \leq \frac{6\ell}{|A|} |F| = \frac{6\ell}{|A|} \deg(P).$$

For each $i = 1, \dots, r$ and each point $x \in E_i$, we have $x \in C_\ell(x_i)$ and so there exist $p_1, \dots, p_\ell, q_1, \dots, q_\ell \in A$ such that $x_i^{p_1 \dots p_\ell} = x^{q_1 \dots q_\ell}$. This gives $H(x_i)^{p_1 \dots p_\ell} = H(x)^{q_1 \dots q_\ell}$, and thus

$$(40) \quad 2^{-\ell} \log H(x_i) \leq \log H(x) \leq 2^\ell \log H(x_i).$$

Combining this with the standard estimates (6) for the height of a polynomial in terms of the height of its roots, and using (39) we deduce that

$$(41) \quad \log H(Q) \leq \deg(Q) + \sum_{x \in E} \log H(x) \leq \frac{6\ell}{|A|} \deg(P) + \sum_{i=1}^r 2^\ell |E_i| \log H(x_i).$$

On the other hand, for each $i = 1, \dots, r$ and each $y \in F_i$, we have $y \in \mathcal{O}(E_i)$ and so there exist $a \in A$ and $x \in E_i$ such that $y = x^a$. Then, we get $H(y) = H(x)^a$, and by (40) we

obtain

$$\log H(y) \geq \frac{M}{2} \log H(x) \geq \frac{M}{2^{\ell+1}} \log H(x_i).$$

Combining this with (6) and using (38), we find

$$\log H(P) + \deg(P) \geq \sum_{y \in F} \log H(y) \geq \sum_{i=1}^r \frac{M}{2^{\ell+1}} |F_i| \log H(x_i) \geq \frac{|A|M}{6\ell 2^{\ell+1}} \sum_{i=1}^r |E_i| \log H(x_i).$$

This provides an upper bound for $\sum_{i=1}^r |E_i| \log H(x_i)$ which after substitution into (41) leads to

$$\log H(Q) \leq \frac{c_1}{|A|M} (M \deg(P) + \log H(P))$$

with $c_1 = \ell 2^{2\ell+4} \geq 6\ell(1 + 2^{2\ell+1})$. This proves the theorem with the constant c replaced by c_1 when P has only simple roots.

In the general case, let m denote the largest multiplicity of a root of P . For $i = 1, \dots, m$, let Z_i denote the set of roots of P having multiplicity at least i , and put $P_i = \prod_{x \in Z_i} (T - x)$. Since roots of P which are conjugate over K have the same multiplicity, P_1, \dots, P_m are polynomials of $K[T]$. Moreover, they have simple roots and P is a constant multiple of their product $P_1 \cdots P_m$. Put $Q_i = \gcd\{P_i(T^a); a \in A\}$ for $i = 1, \dots, m$. We claim that Q is a constant multiple of $Q_1 \cdots Q_m$.

To prove this claim, choose any root x of Q . We first observe that, for each $a \in A$, the multiplicity of x as a root of $P(T^a)$ is the same as the multiplicity of x^a as a root of P (since $T^a - x^a$ has only simple roots). Therefore the multiplicity of x as a root of Q is the largest integer i such that $\mathcal{O}(x) \subseteq Z_i$, or equivalently it is the largest integer i such that x is a root of each of the polynomials Q_1, \dots, Q_i . This being true for each root x of Q shows that Q divides $Q_1 \cdots Q_m$. As the converse is clear, our claim follows.

Since P_1, \dots, P_m all have degree at most n , the above considerations show that the estimates (37) apply to the pair (Q_i, P_i) for each $i = 1, \dots, m$, with c replaced by c_1 . From this we deduce that

$$\deg(Q) = \sum_{i=1}^m \deg(Q_i) \leq \sum_{i=1}^m \frac{6\ell}{|A|} \deg(P_i) = \frac{6\ell}{|A|} \deg(P)$$

and

$$\begin{aligned} \log H(Q) &\leq \deg(Q) + \sum_{i=1}^m \log H(Q_i) \\ &\leq \deg(Q) + \sum_{i=1}^m \frac{c_1}{|A|M} (M \deg(P_i) + \log H(P_i)) \\ &\leq \frac{c_1}{|A|M} ((2M + 1) \deg(P) + \log H(P)), \end{aligned}$$

showing that (37) holds in general with $c = 4c_1$. □

8. PROOF OF THEOREM 1.1 FOR RANK AT LEAST TWO

Let the notation be as in Theorem 1.1, and suppose that $m \geq 2$. For $\sigma = 0$, the result follows from [5, Prop. 1]. So, we may assume that $\sigma > 0$. Define positive constants μ and ϵ by

$$(42) \quad \mu = \frac{m+1}{m+5} \sigma \quad \text{and} \quad \epsilon = \frac{1}{8} \min \left\{ \sigma - \mu, \nu - 1 - \beta + \frac{3m-1}{m+5} \sigma + \tau \right\}.$$

We proceed by contradiction, assuming on the contrary that for each sufficiently large value of n there exists a non-zero polynomial $P \in \mathbb{Z}[T]$ with $\deg(P) \leq n$ and $H(P) \leq \exp(n^\beta)$ satisfying (4). Upon dividing P by its content, we may assume that P is primitive. Fix such an integer n and a corresponding polynomial P . Each computation below assumes that n is larger than an appropriate constant depending only on $\beta, \epsilon, \mu, \sigma, \tau, \nu, \xi_1, \dots, \xi_m$, a condition that we write, in short, as $n \gg 1$. Define

$$t = \left\lceil \frac{n^\tau + 1}{2} \right\rceil, \quad d = \left\lfloor \frac{n}{t} \right\rfloor, \quad \delta = \exp\left(-\frac{n^\nu}{6t}\right), \quad M = [n^\mu], \quad N = [n^\sigma], \quad X = \exp(n^\beta),$$

and factor P as a product $P(T) = T^r \Phi(T)^t P_0(T)$ where r is the largest non-negative integer such that T^r divides $P(T)$, and where Φ is the cyclotomic polynomial of $\mathbb{Z}[T]$ of largest degree such that Φ^t divides P . Since $\nu > 1$, the main condition (28) of Corollary 5.2 is satisfied for $n \gg 1$ and so there exist relatively prime positive integers a_1, \dots, a_m, D with $D \leq (2mn^{2+\sigma})^m$ and a proper subspace U of \mathbb{Q}^m such that we have $|\Phi(\xi_1^{i_1} \cdots \xi_m^{i_m})| \geq \delta$ for any point $(i_1, \dots, i_m) \in \mathbb{Z}^m \setminus U$ with $\max\{|i_1|, \dots, |i_m|\} \leq n^\sigma$ and $\gcd(a_1 i_1 + \cdots + a_m i_m, D) = 1$. If ξ_1, \dots, ξ_m do not all have absolute value one, we can further assume that $a_1 = \cdots = a_m = D = 1$ by applying Proposition 5.3 instead. Define

$$A = \{a \in \mathcal{P} ; M/2 \leq a \leq M \text{ and } a \nmid D\}$$

where \mathcal{P} denotes the set of all prime numbers, and define

$$E = \{\xi_1^{i_1} \cdots \xi_m^{i_m} ; (i_1, \dots, i_m) \in I \setminus (U \cup U')\},$$

where U' denotes the proper subspace of \mathbb{Q}^m generated by all points $(i_1, \dots, i_m) \in \mathbb{Z}^m$ for which $\xi_1^{i_1} \cdots \xi_m^{i_m}$ is algebraic over \mathbb{Q} , and where

$$I = \{(i_1, \dots, i_m) \in \mathbb{Z}^m ; 1 \leq i_1, \dots, i_m \leq n^{\sigma-\mu} \text{ and } \gcd(a_1 i_1 + \cdots + a_m i_m, D) = 1\}.$$

Then, in the notation of Proposition 3.1, we have $\delta_\Phi \geq \delta$ and $\delta_P \leq \exp(-n^\nu)$. We claim that for $n \gg 1$, we also have

$$(43) \quad n^{\mu-\epsilon} \leq |A| \leq n^\mu \quad \text{and} \quad n^{m(\sigma-\mu)-\epsilon} \leq |E| \leq n^{m(\sigma-\mu)}.$$

The upper bounds are clear and the lower bound for $|A|$ comes from the prime number theorem. The lower bound for $|E|$ follows from

$$|E| \geq |I| - |I \cap U| - |I \cap U'| \geq |I| - 2n^{(m-1)(\sigma-\mu)}$$

together with the fact that, by Lemma A.3 (in the appendix), we have $|I| \geq 3n^{m(\sigma-\mu)-\epsilon}$ for $n \gg 1$. In particular, both sets A and E are not empty. The main conditions (10) of Proposition 3.1 also hold for $n \gg 1$ since we have

$$\tau + m(\sigma - \mu) < 1 + \mu \quad \text{and} \quad 1 + \mu < 1 + \sigma \leq \beta.$$

Therefore, according to this proposition, the polynomial

$$Q(T) = \gcd\{P_0^{[j]}(T^a); a \in A, 0 \leq j < t\} \in \mathbb{Z}[T]$$

satisfies

$$\begin{aligned} \prod_{\xi \in E} \frac{|Q(\xi)|}{\text{cont}(Q)} &\leq X^{5Mn/t} \Delta_E^{-t} \left(\frac{\exp(-n^\nu)}{\delta^{3t}} \right)^{|E|} \\ &\leq \exp(15n^{1+\beta+\mu-\tau}) \Delta_E^{-t} \exp(-n^\nu |E|/2) \\ &\leq \exp(15n^{\nu+m(\sigma-\mu)-8\epsilon}) \Delta_E^{-t} \exp(-n^\nu |E|/2). \end{aligned}$$

Since Q is primitive (being a divisor of $P(T^a)$ for any $a \in A$), we conclude from (43) that for $n \gg 1$ we have

$$\prod_{\xi \in E} |Q(\xi)| \leq \exp(-n^\nu |E|/4) \Delta_E^{-t} = \prod_{\xi \in E} \left(\exp(-n^\nu/4) \prod_{\xi' \in E \setminus \{\xi\}} |\xi' - \xi|^{-t/2} \right).$$

Thus, there exists at least one point $\xi \in E$ such that

$$(44) \quad |Q(\xi)| \leq \exp\left(-\frac{n^\nu}{8}\right) \quad \text{or} \quad \prod_{\xi' \in E \setminus \{\xi\}} |\xi' - \xi| \leq \exp\left(-\frac{n^\nu}{4t}\right).$$

Suppose for the moment that the first inequality in (44) holds. Denote by P_1 a divisor of P in $\mathbb{Z}[T]$ of largest degree with no root in $\mathbb{C}_{\text{tor}}^\times \cup \{0\}$, and define

$$Q_1 = \gcd\{P_1(T^a); a \in A\} \in \mathbb{Z}[T].$$

As P_1 divides P in $\mathbb{Z}[T]$, we have $\deg(P_1) \leq n$ and $\log H(P_1) \leq n + \log H(P) \leq 2n^\beta$. Since P_1 has no root in $\mathbb{C}_{\text{tor}}^\times \cup \{0\}$, and since $|A| \geq n^{\mu-\epsilon} \geq n^{\mu/2}$ by (43), Theorem 7.1 applies for $n \gg 1$ with the choice of $\ell = [2/\mu]$, and it gives

$$\deg(Q_1) \leq n^{1-\mu+2\epsilon} \quad \text{and} \quad \log H(Q_1) \leq n^{\beta-2\mu+2\epsilon}.$$

We claim moreover that Q and Q_1 are related by

$$Q = \gcd\{Q_1^{[j]}(T); 0 \leq j < t\}.$$

As Q and Q_1 are primitive, this amounts to showing that their orders of vanishing at any point $z \in \mathbb{C}$ satisfy

$$(45) \quad \text{ord}_z(Q) = \max\{0, \text{ord}_z(Q_1) - t + 1\}.$$

To prove this, we first note that none of P_0 and P_1 vanishes at $z = 0$. So the same is true for Q and Q_1 , and thus both sides of (45) are 0 when $z = 0$. Assume from now on that $z \in \mathbb{C}^\times$. Then we have

$$\text{ord}_z(Q) = \min_{a \in A} \max\{0, \text{ord}_{z^a}(P_0) - t + 1\} \quad \text{and} \quad \text{ord}_z(Q_1) = \min_{a \in A} \text{ord}_{z^a}(P_1).$$

If $z \in \mathbb{C}_{\text{tor}}^\times$, we have $\text{ord}_{z^a}(P_0) < t$ and $\text{ord}_{z^a}(P_1) = 0$ for each $a \in A$, and then both sides of (45) are again equal to 0. Otherwise, we find $\text{ord}_{z^a}(P_0) = \text{ord}_{z^a}(P_1)$ for each $a \in A$, and (45) follows.

The above discussion shows that we may apply Lemma 2.1 to the pair of polynomials Q and Q_1 with the function $\varphi: \mathbb{Z}[T] \rightarrow [0, \infty)$ given by $\varphi(F) = |F(\xi)|$, and the choice of parameters $d = n^{1-\mu+2\epsilon}$, $Y = \exp(n^{\beta-2\mu+2\epsilon})$ and $\delta = \exp(-n^\nu/8)$. Assuming $n \gg 1$, this lemma ensures the existence of a primary polynomial $S \in \mathbb{Z}[T]$ with

$$\deg(S) \leq 4n^{1-\mu-\tau+2\epsilon}, \quad \log H(S) \leq 8n^{\beta-2\mu-\tau+2\epsilon} \quad \text{and} \quad |S(\xi)| \leq \exp(-n^{\nu-\tau-\epsilon}).$$

We have $S(\xi) \neq 0$ since $S \neq 0$ and since ξ is transcendental over \mathbb{Q} (like all the elements of E). Write $\xi = \xi_1^{i_1} \cdots \xi_m^{i_m}$ with exponents in the range $1 \leq i_1, \dots, i_m \leq n^{\sigma-\mu}$. Then $\tilde{S}(T_1, \dots, T_m) = S(T_1^{i_1} \cdots T_m^{i_m})$ is a polynomial of $\mathbb{Z}[T_1, \dots, T_m]$ which for $n \gg 1$ satisfies

$$(46) \quad \begin{aligned} \deg(\tilde{S}) &\leq n^{1+\sigma-2\mu-\tau+3\epsilon}, \\ \log H(\tilde{S}) &\leq n^{\beta-2\mu-\tau+3\epsilon}, \\ 0 &< |\tilde{S}(\xi_1, \dots, \xi_m)| \leq \exp(-n^{\nu-\tau-\epsilon}). \end{aligned}$$

Suppose now that the second inequality holds in (44). Then we have

$$\prod_{\xi' \in E \setminus \{\xi\}} |\xi' - \xi| = \tilde{S}(\xi_1, \dots, \xi_m)$$

with $\tilde{S} \in \mathbb{Z}[T_1, \dots, T_m]$ satisfying $\deg(\tilde{S}) \leq mn^{\sigma-\mu}|E|$, $\log H(\tilde{S}) \leq |E|$ as well as the last inequality of (46) when $n \gg 1$. Since $(m+1)(\sigma-\mu) \leq 1+\sigma-2\mu-\tau$, we deduce that \tilde{S} also fulfills the first two inequalities of (46) when $n \gg 1$.

Therefore the constraints (46) have a solution $\tilde{S} \in \mathbb{Z}[T_1, \dots, T_m]$ for each $n \gg 1$. This contradicts Lemma 2.3 (Gel'fond's criterion) since we have $\beta \geq 1+\sigma$ and since the choice of ϵ in (42) implies

$$\nu - \tau - \epsilon \geq (1 + \sigma - 2\mu - \tau + 3\epsilon) + (\beta - 2\mu - \tau + 3\epsilon) + \epsilon.$$

The proof is complete.

9. AVOIDING CYCLOTOMIC FACTORS IN RANK ONE

The rest of this paper is devoted to the proof of Theorem 1.1 in the case where $m = 1$. In this section, we first establish a measure of approximation of a complex number ξ by roots of unity, under conditions that are sensibly weaker than those of Theorem 1.1. We then prove

two corollaries which finally allow us to push forward the conclusion of Proposition 3.1. The reader who simply wants a proof of Theorem 1.1 in the case where $m = 1$ and $|\xi_1| \neq 1$ can go directly to the remark following those two corollaries and then proceed to Proposition 9.4 at the end of the section.

Proposition 9.1. *Let $\xi \in \mathbb{C}^\times \setminus \mathbb{C}_{\text{tor}}^\times$, and let $\beta, \sigma, \tau, \nu \in \mathbb{R}$ with*

$$\sigma > 0, \quad \tau \geq 0, \quad \sigma + \tau \leq 1 \leq \beta \quad \text{and} \quad \nu > 1 + \beta - \sigma - \tau.$$

Suppose that, for each sufficiently large positive integer n , there exists a non-zero polynomial $P = P_n \in \mathbb{Z}[T]$ with $\deg(P) \leq n$ and $H(P) \leq \exp(n^\beta)$ satisfying

$$\max \{ |P^{[j]}(\xi^i)|; 1 \leq i \leq n^\sigma, 0 \leq j < n^\tau \} \leq \exp(-n^\nu).$$

Then, the ratio $\rho = (\nu - \tau)/(1 - \tau)$ is a real number with $\rho > 1$ and, for each sufficiently large positive integer D and each root of unity Z of order D , we have

$$|\xi - Z| \geq \exp(-\phi(D)^\rho).$$

Proof. We have $\rho > 1$ because $\nu > 1 > \tau$. Now, suppose on the contrary that there exist roots of unity Z of arbitrarily large order D with $|\xi - Z| < \exp(-\phi(D)^\rho)$. Fix such a pair D and Z and put $m = \phi(D)$. By taking D large enough, we may assume that the integer n determined by the condition

$$2n^{1-\tau} < m \leq 2(n+1)^{1-\tau}$$

is arbitrarily large. In particular, we may assume that there exists a corresponding polynomial $P = P_n \in \mathbb{Z}[T]$. Furthermore, we may assume that P is primitive, so that $H(P) = \|P\|$. Let $j \geq 0$ be the smallest non-negative integer such that $P^{(j)}(Z) \neq 0$. Since Z has degree m over \mathbb{Q} , we have $jm \leq \deg(P) \leq n$ and so $j \leq n/m < n^\tau/2$. Consider the polynomial $Q = P^{[j]} \in \mathbb{Z}[T]$. It has degree $\deg(Q) \leq n$ and length $L(Q) \leq (n+1)2^n\|P\| \leq \exp(3n^\beta)$. Since $Q(Z)$ is a non-zero algebraic integer of $\mathbb{Q}(Z)$, its norm from $\mathbb{Q}(Z)$ to \mathbb{Q} is a non-zero integer and so we have

$$(47) \quad 1 \leq \prod_{\substack{1 \leq i \leq D \\ \gcd(i, D)=1}} |Q(Z^i)|$$

Let I denote the set of all integers i coprime to D with $1 \leq i \leq n^\sigma$. Since $D \geq m > 2n^{1-\tau} \geq 2n^\sigma$, this is a subset of the indexing set of the product in the right hand side of (47). For each $i \in I$, we use the Taylor expansion of Q around ξ^i to estimate $|Q(Z^i)|$. Fix such an index i . This gives

$$|Q(Z^i)| \leq \sum_{k=0}^{\infty} |Q^{[k]}(\xi^i)| |\xi^i - Z^i|^k.$$

Since $m > 2n^{1-\tau}$ and $\rho > 1$, we have $|\xi - Z| < \exp(-m^\rho) < \exp(-2n^{\nu-\tau})$. If n is sufficiently large, we also have $\exp(-2n^{\nu-\tau}) \leq n^{-\sigma}$, therefore $|\xi| \leq 1 + n^{-\sigma}$, and so $\max\{1, |\xi|\}^i \leq e$

since $i \leq n^\sigma$. Combining these estimates, we obtain, for n sufficiently large,

$$|\xi^i - Z^i| = |\xi - Z| \left| \sum_{\ell=0}^{i-1} \xi^\ell Z^{i-\ell-1} \right| \leq \exp(-2n^{\nu-\tau}) n^\sigma e \leq \exp(-n^{\nu-\tau}).$$

In particular, we may assume that $|\xi^i - Z^i| \leq 1/2$. On the other hand, since $j < n^\tau/2$, we have $j+k < n^\tau$ for any integer k with $0 \leq k \leq n^\tau/2$, and for such an integer k the hypothesis on P leads to

$$|Q^{[k]}(\xi^i)| = \binom{j+k}{j} |P^{[j+k]}(\xi^i)| \leq 2^n \exp(-n^\nu).$$

For the remaining integers $k > n^\tau/2$, we use instead the crude estimate

$$|Q^{[k]}(\xi^i)| \leq \max\{1, |\xi^i|\}^n L(Q^{[k]}) \leq e^n 2^n L(Q) \leq \exp(5n^\beta).$$

So, putting all together, we find, for each $i \in I$,

$$\begin{aligned} |Q(Z^i)| &\leq 2^n \exp(-n^\nu) \sum_{k=0}^{\lfloor n^\tau/2 \rfloor} |\xi^i - Z^i|^k + \exp(5n^\beta) \sum_{k=\lfloor n^\tau/2 \rfloor+1}^{\infty} |\xi^i - Z^i|^k \\ &\leq 2^{n+1} \exp(-n^\nu) + 2 \exp(5n^\beta) |\xi^i - Z^i|^{n^\tau/2} \\ &\leq 2^{n+1} \exp(-n^\nu) + 2 \exp(5n^\beta - n^\nu/2) \\ &\leq \exp(-n^\nu/3), \end{aligned}$$

where the last step again assumes that n is sufficiently large. For all the other integers i , we use

$$|Q(Z^i)| \leq L(Q) \leq \exp(3n^\beta).$$

Since the inequality (47) involves a product of m factors of the form $|Q(Z^i)|$, including those with $i \in I$, we deduce that

$$(48) \quad 1 \leq \exp(3n^\beta)^m \exp(-n^\nu/3)^{|I|}.$$

Define $\epsilon = (1/2)(\nu - 1 - \beta + \sigma + \tau) > 0$. We have $m \leq 2(n+1)^{1-\tau} \leq 4n^{1-\tau}$, and Lemma A.3 (or the prime number theorem) gives $|I| \geq n^{\sigma-\epsilon}$ for n sufficiently large, since $D = \mathcal{O}(m^2) = \mathcal{O}(n^2)$. Substituting these estimates for m and $|I|$ into (48) leads to a contradiction because $\beta + 1 - \tau < \nu + \sigma - \epsilon$. \square

Corollary 9.2. *Under the notation and hypotheses of Proposition 9.1, there exists a positive integer n_1 with the following property. For each pair of integers n and t with $n \geq n_1$ and $t \geq n^\tau/3$, and for each cyclotomic polynomial $\Phi \in \mathbb{Z}[T]$ whose t -th power Φ^t divides the polynomial $P = P_n$, there exists a positive integer D with $D \leq 2n^3$ such that*

$$(49) \quad \min\{|\Phi(\xi^i)|; 1 \leq i \leq n^\sigma, \gcd(i, D) = 1\} \geq \exp\left(-\frac{n^\nu}{6t}\right).$$

Proof. Choose $\epsilon > 0$ such that $\nu - \epsilon > 1 + \beta - \sigma - \tau$. Then the hypotheses of Proposition 9.1 remain satisfied with the parameter ν replaced by $\nu - \epsilon$, and so there exists a constant $c > 0$ such that, for any integer $D \geq 1$ and any root of unity Z of order D , we have

$$(50) \quad |\xi - Z| \geq \exp(-c\phi(D)^{\tilde{\rho}}) \quad \text{where} \quad \tilde{\rho} = \frac{\nu - \epsilon - \tau}{1 - \tau}.$$

Let n be a positive integer for which the polynomial $P = P_n$ is defined, let t be an integer with $t \geq n^\tau/3$, and let Φ be a cyclotomic polynomial of $\mathbb{Z}[T]$ such that Φ^t divides P . We may assume that Φ is non-constant, and so we have $t \leq n$. Then, for n sufficiently large, all conditions of Proposition 4.1 are satisfied with $m = 1$, $\xi_1 = \xi$ and the choice of parameters $d = [n/t]$, $\delta = \exp(-n^\nu/(6t))$ and $N = [n^\sigma]$ (the condition (14) holds since $\nu > 1$). So, there exist relatively prime positive integers a_1 and D with $D \leq 2(n/t)^2 n^\sigma \leq 2n^3$ such that either (49) holds or there exists a root Z of Φ which has order D as a root of unity and satisfies

$$(51) \quad |\xi - Z^{a_1}|^G \leq \exp\left(-\frac{n^\nu}{12t}\right)$$

where G denotes the multiplicity of Z as a root of Φ . Suppose that the second eventuality holds. We will see that, in this case, the integer n is bounded and this will complete the proof. Since Z and Z^{a_1} are conjugate over \mathbb{Q} (they have the same order D), we may assume without loss of generality that $a_1 = 1$. Then, by comparing (50) and (51), we find

$$(52) \quad cG\phi(D)^{\tilde{\rho}} \geq \frac{n^\nu}{12t}.$$

However, since Z has degree $\phi(D)$ over \mathbb{Q} , we also have $G\phi(D) \leq \deg(\Phi) \leq n/t$. Combining this with (52), we get $12c\phi(D)^{\tilde{\rho}-1} \geq n^{\nu-1}$. Finally, since $\phi(D) \leq n/t \leq 3n^{1-\tau}$, this gives $n \leq (12c3^{\tilde{\rho}-1})^{1/\epsilon}$. \square

Corollary 9.3. *Let the notation and hypotheses be as in Proposition 9.1, and let $\mu \in \mathbb{R}$ with $0 < \mu \leq 1 - \tau$ and $2\mu + \tau < \nu$. Then, there exists a positive integer n_2 with the following property. For each integer $n \geq n_2$ and each non-empty subset I of $\{1, 2, \dots, [n^\mu]\}$, the set $E = \{\xi^i; i \in I\}$ satisfies*

$$\Delta_E \geq \exp\left(-\frac{1}{4}n^{\nu-\tau}|E|\right).$$

Proof. Again, choose $\epsilon > 0$ such that $\nu - \epsilon > 1 + \beta - \sigma - \tau$. Arguing as in the proof of Corollary 9.2, we find that there is a constant $c > 0$ such that (50) holds for any integer $D \geq 1$ and any root of unity Z of order D . Let n be a positive integer and let $E = \{\xi^i; i \in I\}$ for some non-empty subset I of $\{1, 2, \dots, [n^\mu]\}$. Suppose that $\Delta_E < \exp(-(1/4)n^{\nu-\tau}|E|)$. We need to show that n is bounded (independently of the choice of I). By definition, we have $\Delta_E = \prod_{i < j} |\xi^i - \xi^j|$ where the product runs through all pairs (i, j) of elements of I with $i < j$. This means that we can write $\Delta_E = |\xi|^r |\Phi(\xi)|$ for an integer r with $0 \leq r \leq n^{2\mu}|E|$

and a cyclotomic polynomial Φ of $\mathbb{Z}[T]$ of degree at most $n^{2\mu}|E|$. Applying Lemma 4.4, we deduce that some root Z of Φ satisfies

$$|\xi - Z|^G \leq \exp(n^{2\mu}|E| \log(c_1(n^{3\mu})^4) - (1/4)n^{\nu-\tau}|E|),$$

where $c_1 = 2 \max\{1, |\xi|^{-1}\}$ and where G denotes the multiplicity of Z as a root of Φ . Since $\nu - \tau > 2\mu$, we conclude that for n large enough we have

$$(53) \quad |\xi - Z|^G \leq \exp(-(1/8)n^{\nu-\tau}|E|).$$

Now, let D denote the order of Z as a root of unity. Combining this estimate with (50), we obtain

$$(54) \quad 8cG\phi(D)^{\tilde{\rho}} \geq n^{\nu-\tau}|E|.$$

On the other hand, because of the actual definition of Φ , we have $D \leq n^\mu$, and G is the number of pairs of elements (i, j) of I with $i < j$ and $i \equiv j \pmod{D}$. Thus, we also have $G \leq n^\mu|E|/D$. Substituting this upper bound for G into (54) and using $\phi(D) \leq D$, we obtain $8cD^{\tilde{\rho}-1} \geq n^{\nu-\mu-\tau}$. Finally, since $D \leq n^\mu \leq n^{1-\tau}$, this leads to $8cn^{\nu-1-\epsilon} \geq n^{\nu-\mu-\tau}$, thus $8c \geq n^{1+\epsilon-\mu-\tau} \geq n^\epsilon$ and so $n \leq (8c)^{1/\epsilon}$. \square

Remark. If we assume that $|\xi| \neq 1$, then for each cyclotomic polynomial $\Phi \in \mathbb{Z}[T]$ and each non-zero integer i , we find

$$|\Phi(\xi^i)| \geq |1 - |\xi^i||^{\deg(\Phi)} \geq c_1^{\deg(\Phi)},$$

where $c_1 = 1 - \min\{|\xi|, |\xi|^{-1}\}$. Since $\nu > 1$, we deduce that, in this case, Corollary 9.2 holds with $D = 1$. Moreover, for a set E as in Corollary 9.3, we have $\Delta_E = |\xi|^r \Phi(\xi)$ where r is an integer with $0 \leq r \leq n^{2\mu}|E|$ and Φ is a cyclotomic polynomial of $\mathbb{Z}[T]$ with $\deg(\Phi) \leq n^{2\mu}|E|$, and thus $\Delta_E \geq \exp(c_2 n^{2\mu}|E|)$ where $c_2 = \log(c_1 \min\{1, |\xi|\})$, which is stronger than the conclusion of Corollary 9.3.

The main result of this section is the following.

Proposition 9.4. *Let $\xi \in \mathbb{C}^\times \setminus \mathbb{C}_{\text{tor}}^\times$, and let $\beta, \epsilon, \mu, \sigma, \tau, \nu \in \mathbb{R}$ with*

$$0 < \mu < \sigma, \quad 0 \leq \tau \leq 1 - \sigma, \quad \beta > \max\{1 + \sigma - \mu, 2\mu + \tau\},$$

$$0 < 2\epsilon < \min\{\mu, \sigma - \mu\} \quad \text{and} \quad \nu > 1 + \beta + \sigma - 2\mu - \tau + 2\epsilon.$$

Suppose that for each sufficiently large positive integer n , there exists a non-zero polynomial $P = P_n \in \mathbb{Z}[T]$ with $\deg(P) \leq n$ and $H(P) \leq \exp(n^\beta)$ satisfying

$$\max\{|P^{[j]}(\xi^i)|; 1 \leq i \leq n^\sigma, 0 \leq j < n^\tau\} < \exp(-n^\nu).$$

Then, for each large enough index n , there exists an integer D with $1 \leq D \leq 2n^3$ satisfying the following property. For any set I of cardinality $|I| \geq n^{\mu-\epsilon}$ consisting of integers i coprime

to D in the range $1 \leq i \leq n^\mu$, there exists a primary polynomial $S \in \mathbb{Z}[T]$ satisfying

$$(55) \quad \deg(S) \leq n^{1-(\sigma-\mu)-\tau+3\epsilon}, \quad \log H(S) \leq n^{\beta-2(\sigma-\mu)-\tau+3\epsilon}, \quad \prod_{i \in I} |S(\xi^i)| \leq \exp(-n^{\nu+\mu-\tau-2\epsilon}).$$

Proof. Fix a large integer n and a corresponding polynomial P . Without loss of generality, we may assume that P is primitive. Put $t = \lfloor (n^\tau + 1)/2 \rfloor$, and write $P(T)$ as a product $P(T) = T^r \Phi(T)^t P_0(T)$, where r is the largest positive integer such that T^r divides P and Φ is the cyclotomic polynomial of $\mathbb{Z}[T]$ of largest degree such that Φ^t divides P . Assuming n large enough, Corollary 9.2 shows that (49) holds for some integer D with $1 \leq D \leq 2n^3$. Let I be a subset of $\{i \in \mathbb{Z}; 1 \leq i \leq n^\mu, \gcd(i, D) = 1\}$ with cardinality $|I| \geq n^{\mu-\epsilon}$ (such a subset exists if n is large enough), and define $E = \{\xi^i; i \in I\}$. Put also $M = \lfloor n^{\sigma-\mu} \rfloor$ and define A to be the set of all prime numbers p not dividing D with $M/2 \leq p \leq M$. Finally, set $X = \exp(n^\beta)$ so that $H(P) \leq X$. Then, in the notation of Proposition 3.1, we have

$$c_E \leq \exp(c_1 n^\mu), \quad \delta_\Phi \geq \exp\left(-\frac{n^\nu}{6t}\right) \quad \text{and} \quad \delta_P \leq \exp(-n^\nu),$$

where $c_1 = \log \max\{|\xi|, |\xi|^{-1}\}$. Since $\xi \notin \mathbb{C}_{\text{tor}}^\times \cup \{0\}$, the sets E and I have the same cardinality. Assuming n large enough, we have

$$n^{\sigma-\mu-\epsilon} \leq |A| \leq n^{\sigma-\mu} \quad \text{and} \quad n^{\mu-\epsilon} \leq |E| = |I| \leq n^\mu$$

and the main condition (10) of Proposition 3.1 holds because $\tau + \mu < 1 + \sigma - \mu < \beta$ and $2\mu + \tau < \beta$. Combining this proposition with Corollary 9.3, it follows that the polynomial

$$Q(T) = \gcd\{P_0^{[j]}(T^a); a \in A, 0 \leq j < t\} \in \mathbb{Z}[T]$$

satisfies

$$\begin{aligned} \prod_{i \in I} |Q(\xi^i)| &\leq \exp\left(\frac{5}{t} n^{1+\beta+\sigma-\mu}\right) \Delta_E^{-t} \exp\left(-\frac{n^\nu}{2} |E|\right) \\ &\leq \exp(15n^{1+\beta+\sigma-\mu-\tau}) \exp\left(-\frac{n^\nu}{4} |E|\right) \\ &\leq \exp(-(1/8)n^{\nu+\mu-\epsilon}) \end{aligned}$$

provided that n is large enough.

Denote by P_1 a divisor of P in $\mathbb{Z}[T]$ of largest degree with no root in $\mathbb{C}_{\text{tor}}^\times \cup \{0\}$, and define

$$Q_1 = \gcd\{P_1(T^a); a \in A\} \in \mathbb{Z}[T].$$

Applying Theorem 7.1 as in Section 8, upon noting that $\beta \geq 1 + \sigma - \mu$, we find that for n sufficiently large we have

$$\deg(Q_1) \leq n^{1-(\sigma-\mu)+2\epsilon} \quad \text{and} \quad \log H(Q_1) \leq n^{\beta-2(\sigma-\mu)+2\epsilon}.$$

As in Section 8, we also note that $Q = \gcd\{Q_1^{[j]}(T); 0 \leq j < t\}$. This means that we may apply Lemma 2.1 to the pair of polynomials Q and Q_1 with the function $\varphi: \mathbb{Z}[T] \rightarrow [0, \infty)$

given by $\varphi(F) = \prod_{i \in I} |F(\xi^i)|$, and the choice of parameters

$$d = n^{1-(\sigma-\mu)+2\epsilon}, \quad Y = \exp(n^{\beta-2(\sigma-\mu)+2\epsilon}) \quad \text{and} \quad \delta = \exp(-(1/8)n^{\nu+\mu-\epsilon}).$$

Assuming n large enough, this lemma ensures the existence of a primary polynomial $S \in \mathbb{Z}[T]$ with the required properties (55). \square

10. AN ESTIMATE RELATED TO ZARANKIEWICZ PROBLEM

The following result is a strengthening of Proposition 9.1 of [7]. As the latter, it has connection with a well-known combinatorial problem of Zarankiewicz (see [3, Chap. 12]).

Proposition 10.1. *Let A and B be finite non-empty sets, let κ_1 and κ_2 be positive real numbers, and let $\varphi: A \times B \rightarrow [0, \kappa_1]$ be any function on $A \times B$ with values in the interval $[0, \kappa_1]$. Suppose that the inequality*

$$\sum_{b \in B} \min\{\varphi(a_1, b), \varphi(a_2, b)\} \leq \kappa_2$$

holds for any pair of distinct elements a_1 and a_2 of A . Then, we have

$$\sum_{a \in A} \sum_{b \in B} \varphi(a, b) \leq \max\{|A|\sqrt{2|B|\kappa_1\kappa_2}, 2|B|\kappa_1\}.$$

The connection with the problem of Zarankiewicz is the following. For positive integers m and n , an $m \times n$ matrix M with coefficients in $\{0, 1\}$ can be viewed as a function $\varphi: A \times B \rightarrow \{0, 1\}$ where $A = \{1, \dots, m\}$ and $B = \{1, \dots, n\}$. If, for some integer $n_1 \geq 1$, the matrix M contains no $2 \times n_1$ sub-matrix consisting entirely of ones, the hypotheses of the proposition are satisfied with $\kappa_1 = 1$ and $\kappa_2 = n_1 - 1$ and consequently this matrix contains at most $\max\{m\sqrt{2n(n_1 - 1)}, 2n\}$ ones.

Proof. We first claim that for each $i = 1, \dots, |A|$, we have

$$(56) \quad \sum_{a \in A} \sum_{b \in B} \varphi(a, b) \leq \frac{|A||B|}{i} \kappa_1 + \frac{(i-1)|A|}{2} \kappa_2.$$

In the case where $i = |A|$, this follows from Proposition 9.1 of [7]. The proof of the general case proceeds by reduction to this situation. Put $m = |A|$ and, for each $a \in A$, define $\psi(a) = \sum_{b \in B} \varphi(a, b)$. Choose also an ordering $\{a_1, a_2, \dots, a_m\}$ of the elements of A such that $\psi(a_1) \geq \psi(a_2) \geq \dots \geq \psi(a_m)$, and consider the set $A' = \{a_1, \dots, a_i\}$. Then, A' and B satisfy all the hypotheses of the proposition for the restriction of φ to $A' \times B$, with the same values of κ_1 and κ_2 . Accordingly, by [7, Prop. 9.1], we have

$$\sum_{a \in A'} \psi(a) = \sum_{a \in A'} \sum_{b \in B} \varphi(a, b) \leq |B|\kappa_1 + \binom{i}{2} \kappa_2.$$

On the other hand, since $\psi(a_j) \leq (1/i) \sum_{a \in A'} \psi(a)$ for each $j = i + 1, \dots, m$, we also find

$$\sum_{a \in A} \sum_{b \in B} \varphi(a, b) = \sum_{a \in A} \psi(a) \leq \left(1 + \frac{m-i}{i}\right) \sum_{a \in A'} \psi(a) = \frac{|A|}{i} \sum_{a \in A'} \psi(a).$$

Our claim (56) follows by combining these two estimates.

To conclude, put $\rho = 2|B|\kappa_1/\kappa_2$. If $\rho < |A|^2$, we apply (56) with $i = \lfloor \sqrt{\rho} \rfloor + 1$. This gives

$$\sum_{a \in A} \sum_{b \in B} \varphi(a, b) \leq \frac{|A||B|}{\sqrt{\rho}} \kappa_1 + \frac{|A|\sqrt{\rho}}{2} \kappa_2 = |A|\sqrt{\rho} \kappa_2 = |A|\sqrt{2|B|\kappa_1\kappa_2}.$$

If $\rho \geq |A|^2$, the same inequality with $i = |A|$ leads to

$$\sum_{a \in A} \sum_{b \in B} \varphi(a, b) \leq |B|\kappa_1 + \frac{|A|^2}{2} \kappa_2 \leq |B|\kappa_1 + \frac{\rho}{2} \kappa_2 = 2|B|\kappa_1.$$

The proof is complete. \square

11. PRODUCTS OF VALUES OF POLYNOMIALS AT POWERS OF ξ

In this section, we use Proposition 10.1 to prove a transcendence criterion for a complex number ξ , based on products of values of polynomials at powers of ξ . Then we combine this criterion with Proposition 9.4 to complete the proof of Theorem 1.1 in the case $m = 1$.

Theorem 11.1. *Let $\xi \in \mathbb{C}$ be a transcendental number, and let $\alpha, \beta, \mu, \omega \in \mathbb{R}$ with*

$$(57) \quad \alpha \geq \mu > 0, \quad \beta \geq \alpha + \mu \quad \text{and} \quad \omega > \alpha + \beta + (3/2)\mu.$$

For infinitely many positive integers n , there exists no primary polynomial $Q \in \mathbb{Z}[T]$ without root in $\mathbb{C}_{\text{tor}}^\times \cup \{0\}$ satisfying

$$(58) \quad \deg(Q) \leq n^\alpha, \quad H(Q) \leq \exp(n^\beta) \quad \text{and} \quad \prod_{a \in A} \prod_{b \in B} |Q(\xi^{ab})| \leq \exp(-n^\omega),$$

for some non-empty subsets A and B of $\{1, 2, \dots, \lfloor n^{\mu/2} \rfloor\}$.

Proof. We proceed by contradiction, assuming on the contrary that such a triple (Q, A, B) exists for each sufficiently large n . Fix an appropriate integer n , and define $E = \{\xi^b; b \in B\}$ for a corresponding choice of (Q, A, B) . Note that Q is primitive being primary and non-constant, thus $H(Q) = \|Q\|$. We consider two cases according to the size of Δ_E (see §2 for the definition of this quantity).

Case 1: $\Delta_E^{-1} \leq \exp((1/4)n^{\omega-\mu})$.

We claim that, if n is sufficiently large, there exists $(a, b) \in A \times B$ such that $|Q(\xi^{ab})| \leq \exp(-(1/2)n^{\omega-\mu/2})$. To prove this, we first note that, for each $(a, b) \in A \times B$, we have

$$|Q(\xi^{ab})| \leq \|Q\| \exp(c_1 n^{\alpha+\mu}) \leq \exp((c_1 + 1)n^\beta),$$

where $c_1 = \log(1 + |\xi|)$, so that we can write

$$|Q(\xi^{ab})| = \exp((c_1 + 1)n^\beta - \varphi(a, b))$$

for some real number $\varphi(a, b) \geq 0$. This defines a function $\varphi: A \times B \rightarrow [0, \infty)$ which, by the last condition of (58), satisfies

$$(59) \quad \sum_{a \in A} \sum_{b \in B} \varphi(a, b) \geq n^\omega.$$

We also note that, for distinct elements a_1 and a_2 of A , the polynomials $Q(T^{a_1})$ and $Q(T^{a_2})$ are relatively prime in $\mathbb{Z}[T]$. This is because, they are primitive polynomials of $\mathbb{Z}[T]$ and, if z is a common root of them, then z^{a_1} and z^{a_2} are roots of $Q(T)$. However, since $Q(T)$ is a primary polynomial of $\mathbb{Z}[T]$, its roots are conjugate over \mathbb{Q} . So, there exists an automorphism σ of the splitting field of $Q(T)$ over \mathbb{Q} such that $\sigma(z^{a_1}) = z^{a_2}$. Then, upon denoting by m the order of σ , we find $z^{a_1^m} = \sigma^m(z^{a_1}) = z^{a_2^m}$. Since $a_1^m \neq a_2^m$, this implies that $z \in \mathbb{C}_{\text{tor}}^\times \cup \{0\}$, contrary to the assumption that $Q(T)$ has no root in that set. Thus, the gcd of $Q(T^{a_1})$ and $Q(T^{a_2})$ in $\mathbb{Z}[T]$ is 1.

We apply Proposition 2.2 to the above situation with $t = 1$, $r = 2$ and $P_i(T) = Q(T^{a_i})$ for $i = 1, 2$. Since both polynomials P_1 and P_2 have degree $\leq n^{\alpha+\mu/2}$ and height $\leq \exp(n^\beta)$, and since we assume that $\Delta_E^{-1} \leq \exp((1/4)n^{\omega-\mu})$, it gives

$$\begin{aligned} 1 &\leq \exp(10n^{2\alpha+\mu} + c_2n^{\alpha+3\mu/2} + (1/4)n^{\omega-\mu} + 2n^{\beta+\alpha+\mu/2}) \\ &\quad \times \prod_{b \in B} \max \{ \exp((c_1 + 1)n^\beta - \varphi(a_1, b)), \exp((c_1 + 1)n^\beta - \varphi(a_2, b)) \} \end{aligned}$$

where $c_2 = 4\log(2 + |\xi|)$. By (57), the exponent $\omega - \mu$ exceeds all the other exponents of powers of n in the first factor on the right. So, if n is sufficiently large, we deduce that

$$\sum_{b \in B} \min \{ \varphi(a_1, b), \varphi(a_2, b) \} \leq \frac{1}{2}n^{\omega-\mu}.$$

This means that Proposition 10.1 applies to the function φ with κ_1 equals to the largest value of φ on $A \times B$, and with $\kappa_2 = (1/2)n^{\omega-\mu}$. Because of (59), this implies that

$$n^\omega \leq \max \{ n^{\mu/2} \sqrt{n^{\omega-\mu/2} \kappa_1}, 2n^{\mu/2} \kappa_1 \},$$

and so $\kappa_1 \geq (1/2)n^{\omega-\mu/2}$. Thus, there exists $(a, b) \in A \times B$ such that

$$|Q(\xi^{ab})| \leq \exp((c_1 + 1)n^\beta - (1/2)n^{\omega-\mu/2}).$$

If n is sufficiently large, this means that $|Q(\xi^{ab})| \leq \exp(-(1/4)n^{\omega-\mu/2})$, thereby proving our claim. For such a choice of (a, b) , the polynomial $S(T) = Q(T^{ab}) \in \mathbb{Z}[T]$ satisfies

$$(60) \quad \deg(S) \leq n^{\alpha+\mu}, \quad H(S) \leq \exp(n^\beta) \quad \text{and} \quad 0 < |S(\xi)| \leq \exp(-(1/4)n^{\omega-\mu/2}).$$

Case 2: $\Delta_E^{-1} > \exp((1/4)n^{\omega-\mu})$.

In this situation, we define

$$S(T) = \prod_{\substack{b, b' \in B \\ b < b'}} |T^{b'} - T^b|^u \quad \text{where} \quad u = \lfloor n^{\mu/2} \rfloor + 1.$$

This polynomial of $\mathbb{Z}[T]$ fulfills the inequalities (60) because

$$\deg(S) \leq \binom{|B|}{2} n^{\mu/2} u \leq n^{2\mu} \leq n^{\alpha+\mu}, \quad \log H(S) \leq \binom{|B|}{2} u \log(2) \leq n^{3\mu/2} \leq n^\beta,$$

and, by definition of Δ_E , we have $0 < |S(\xi)| = \Delta_E^u \leq \exp(-(1/4)n^{\omega-\mu/2})$.

Thus, in both cases, the conditions (60) have a solution $S(T) \in \mathbb{Z}[T]$ for n sufficiently large. By Gel'fond's criterion (Lemma 2.3), this is impossible because $\beta \geq \alpha + \mu$ and $\omega - \mu/2 > (\alpha + \mu) + \beta$. \square

Proof of Theorem 1.1 in the case $m = 1$. Suppose that the hypotheses of Theorem 1.1 are satisfied for $m = 1$. For $\sigma = 0$, the result follows from [5, Prop. 1]. We may therefore assume that $\sigma > 0$. Arguing by contradiction, we also assume that, for each sufficiently large positive integer n , there exists a non-zero polynomial $P \in \mathbb{Z}[T]$ with $\deg(P) \leq n$ and $H(P) \leq \exp(n^\beta)$ satisfying (4). Put $\xi = \xi_1$ and $\mu = (8/11)\sigma$. Then, the conditions of Proposition 9.4 are fulfilled for any choice of $\epsilon > 0$ small enough as a function of β, σ, τ, ν . For each sufficiently large n and for the corresponding integer D with $1 \leq D \leq 2n^3$ provided by Proposition 9.4, consider the set of all prime numbers p not dividing D in the interval $1 < p \leq n^{\mu/2}$, and partition this set into two disjoint subsets A and B of cardinality at least $n^{(\mu-\epsilon)/2}$. Then, the set $I = \{ab; a \in A, b \in B\}$ has cardinality $|I| = |A||B| \geq n^{\mu-\epsilon}$ and consists of integers coprime to D from the interval $[1, n^\mu]$. So, Proposition 9.4 provides us with a primary polynomial $S \in \mathbb{Z}[T]$ satisfying the conditions (55). This contradicts Theorem 11.1 if, from the start, we choose ϵ small enough so that the conditions (57) hold with $\alpha = 1 - (\sigma - \mu) - \tau + 3\epsilon$, $\omega = \nu + \mu - \tau - 2\epsilon$, and β replaced by $\beta - 2(\sigma - \mu) - \tau + 3\epsilon$. \square

APPENDIX A. COUNTING LEMMAS

The purpose of this appendix is to provide an estimate that is needed in §8 in the course of the proof of the main Theorem 1.1 for the case $m \geq 2$. It concerns the cardinality of certain subsets of \mathbb{Z}^m which arise from an application of Corollary 5.2. I believe that this has appeared elsewhere but as I have been unable to find a suitable reference, I include the details of proof for the convenience of the reader. It starts with a preliminary lemma.

Lemma A.1. *Let $m, d, N \in \mathbb{N}^*$, and let $a_1, \dots, a_m, b \in \mathbb{Z}$ with $\gcd(a_1, \dots, a_m, d) = 1$. Then, the set*

$$I = \{(i_1, \dots, i_m) \in \mathbb{Z}^m; 1 \leq i_1, \dots, i_m \leq N \text{ and } a_1 i_1 + \dots + a_m i_m \equiv b \pmod{d}\}$$

has cardinality $|I| = N^m/d + E$ with an error E satisfying $|E| \leq (3N)^{m-1}$.

The crucial point here is that the error term depends only on m and N .

Proof. If $m = 1$, the set I is the intersection of $\{1, 2, \dots, N\}$ with an arithmetic progression with difference d . Therefore, its cardinality is either $[N/d]$ or $[N/d] + 1$, and so we have $||I| - N/d| \leq 1$. Suppose now that $m \geq 2$. Write $d_1 = \gcd(a_1, d)$, $d' = d/d_1$ and $a' = a_1/d_1$, and define

$$I' = \{(i_2, \dots, i_m) \in \mathbb{Z}^{m-1}; 1 \leq i_2, \dots, i_m \leq N \text{ and } a_2 i_2 + \dots + a_m i_m \equiv b \pmod{d_1}\}.$$

For any point $(i_1, \dots, i_m) \in \mathbb{Z}^m$ we have $(i_1, \dots, i_m) \in I$ if and only if $(i_2, \dots, i_m) \in I'$ and

$$(61) \quad a' i_1 \equiv (b - a_2 i_2 - \dots - a_m i_m)/d_1 \pmod{d'} \quad \text{with } 1 \leq i_1 \leq N.$$

By the preceding considerations (case $m = 1$), for fixed $(i_2, \dots, i_m) \in I'$ the set of solutions i_1 of (61) has cardinality $N/d' + E(i_2, \dots, i_m)$ with $|E(i_2, \dots, i_m)| \leq 1$. From this we deduce that

$$|I| = \sum_{(i_2, \dots, i_m) \in I'} \left(\frac{N}{d'} + E(i_2, \dots, i_m) \right) = \frac{N}{d'} |I'| + E' \quad \text{with } |E'| \leq |I'|.$$

Since $\gcd(a_2, \dots, a_m, d_1) = 1$, we can also assume by induction that $|I'| = N^{m-1}/d_1 + E''$ with $|E''| \leq (3N)^{m-2}$. Combining these estimates gives $|I| = N^m/d + E$ with

$$|E| \leq |I'| + N|E''| \leq N^{m-1} + (N+1)(3N)^{m-2} \leq (3N)^{m-1}.$$

□

The main estimate is the following.

Lemma A.2. *Let $m, D, N \in \mathbb{N}^*$, and let $a_1, \dots, a_m \in \mathbb{Z}$ with $\gcd(a_1, \dots, a_m, D) = 1$. Then,*

$$I = \{(i_1, \dots, i_m) \in \mathbb{Z}^m; 1 \leq i_1, \dots, i_m \leq N \text{ and } \gcd(a_1 i_1 + \dots + a_m i_m, D) = 1\}$$

has cardinality

$$|I| = N^m \prod_{p|D} \left(1 - \frac{1}{p}\right) + E \quad \text{with } |E| \leq 2^{\omega(D)} (3N)^{m-1},$$

where the product runs over all prime factors p of D and where $\omega(D)$ stands for the number of distinct prime factors of D .

Proof. For each positive divisor d of D , define

$$I_d = \{(i_1, \dots, i_m) \in \mathbb{Z}^m; 1 \leq i_1, \dots, i_m \leq N \text{ and } d | a_1 i_1 + \dots + a_m i_m\}.$$

Since $\gcd(a_1, \dots, a_m, d) = 1$, the preceding lemma gives $|I_d| = N^m/d + E_d$ with $|E_d| \leq (3N)^{m-1}$. In terms of the Moebius function μ , the inclusion-exclusion principle gives

$$|I| = \sum_{d|D} \mu(d) |I_d|.$$

The conclusion then follows from the fact that $\sum_{d|D} \mu(d) d^{-1} = \prod_{p|D} (1 - p^{-1})$ and that D admits exactly $2^{\omega(D)}$ square-free positive divisors. □

In the present paper, we use the estimate of the above lemma in the following form.

Lemma A.3. *Let the notation be as in Lemma A.2, and let ϵ and κ be positive real numbers such that $D \leq N^\kappa$. If N is sufficiently large in terms of ϵ , κ and m , then the set I has cardinality at least $N^{m-\epsilon}$.*

Proof. By Lemma A.2, we have $|I| \geq N^m 2^{-\omega(D)} - 2^{\omega(D)} (3N)^{m-1}$. Since $2^{\omega(D)} = \mathcal{O}(D^\delta)$ for any fixed $\delta > 0$ (see [4, Thm 315]), we also find that $2^{\omega(D)} \leq 2^{\omega(D)} 3^{m-1} \leq (1/2)N^\epsilon$ if N is sufficiently large in terms of ϵ , κ and m . As we may assume that $\epsilon \leq 1/2$, this gives $|I| \geq 2N^{m-\epsilon} - (1/2)N^{m-1+\epsilon} \geq N^{m-\epsilon}$. \square

REFERENCES

- [1] W. D. Brownawell, Sequences of Diophantine approximations, *J. Number Theory* **6** (1974), 11–21.
- [2] C. Chevalley, *Introduction to the theory of algebraic functions of one variable*, American Math. Soc., 1951.
- [3] P. Erdős and J. Spencer *Probabilistic methods in combinatorics*, Probability and Mathematical Statistics **17**, Academic Press, 1974.
- [4] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, fifth edition, Clarendon Press, Oxford, 1985.
- [5] M. Laurent and D. Roy, Criteria of algebraic independence with multiplicities and interpolation determinants, *Trans. Amer. Math. Soc.* **351** (1999), 1845–1870.
- [6] D. Roy, An arithmetic criterion for the values of the exponential function, *Acta Arith.* **97** (2001), 183–194.
- [7] D. Roy, Small value estimates for the additive group, *Intern. J. Number Theory*, **6** (2010), 919–956; arXiv:0708.2307v1 [math.NT].
- [8] W. M. Schmidt, *Diophantine approximation*, Lecture Note in Math., vol. 785, Springer-Verlag, 1980.
- [9] M. Waldschmidt, Solution du huitième problème de Schneider, *J. Number Theory* **5** (1973), 191–202.

DÉPARTEMENT DE MATHÉMATIQUES, UNIVERSITÉ D'OTTAWA, 585 KING EDWARD, OTTAWA, ONTARIO K1N 6N5, CANADA

E-mail address: droy@uottawa.ca